Theory and Practice of Asset Protection

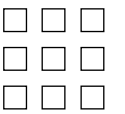
SECURITY SUPERVISION & MANAGEMENT

International Foundation for Protection Officers

Edited by Sandi J. Davies
and Christopher A. Hertig, CPP, CPOI

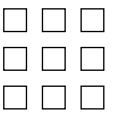
THIRD EDITION

BH



Security Supervision and Management

This page intentionally left blank



Security Supervision and Management

The Theory and Practice of Asset Protection

Third Edition

International Foundation for Protection Officers

Edited by

Sandi J. Davies and

Christopher A. Hertig, CPP, CPOI

AMSTERDAM • BOSTON • HEIDELBERG • LONDON • NEW YORK • OXFORD

PARIS • SAN DIEGO • SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Butterworth-Heinemann is an imprint of Elsevier

Acquisitions Editor: Pamela Chester
Publisher: Amorette Pedersen
Marketing Manager: Marissa Hederson
Project Manager: Murthy Karthikeyan
Cover Designer: Joanne Blank
Compositor: SPI Technologies India Pvt. Ltd.

Butterworth-Heinemann is an imprint of Elsevier
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA
Linacre House, Jordan Hill, Oxford OX2 8DP, UK

First edition 1995
Second edition 1999
Third edition 2008

Library of Congress Cataloging-in-Publication Data
Security supervision and management: theory and practice of asset protection/edited by Sandi J. Davies and Christopher A. Hertig. –3rd ed.
p. cm.
Rev. ed. of: Security supervision. 2nd ed.
ISBN-13: 978-0-7506-8436-1
ISBN-10: 0-7506-8436-4
1. Police, Private–Training of–Handbooks, manuals, etc. 2. Police, Private–Management–Handbooks, manuals, etc. 3. Private security services–Handbooks, manuals, etc. 4. Private security services–Management–Handbooks, manuals, etc. I. Davies, Sandi J. II. Hertig, Christopher A. III. Security supervision.
HV8290.S39 2008
363.28′90683–dc22 2007034075

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

ISBN: 978-0-7506-8436-1

For information on all Butterworth–Heinemann publications visit our Web site at www.books.elsevier.com

08 09 10 11 12 13 9 8 7 6 5 4 3 2 1

Printed in the United States of America.

Cover photos © Jupiter images and istockphoto.

Table of Contents

Writers' Gallery

Michael J. Apgar, CSSM, CPO

Mike is a police officer with a background in emergency medicine. He has worked in campus, hospital, and nuclear security environments. Mr. Apgar is a graduate of York College of Pennsylvania where he majored in criminal justice. He is Certified in Security Supervision and Management (CSSM) and is also a Certified Protection Officer (CPO).

Daniel R. Baker, Ph.D.

Dan is currently a teacher educator in the College of Education, School of Occupational and Adult Education, Oklahoma State University. He is a graduate of the School of Public Administration at the University of Southern California and holds an advanced graduate certificate in Police Administration. With 25 years of protection experience, he holds instructor certifications in security and law enforcement from Oklahoma Council on Law Enforcement Education and Training.

Colin Best, CPO

Colin Best's experience in the security industry dates back to the mid-1980s. Colin was employed by Petro-Canada Inc. for 10 years in a security supervisory role specializing in security systems. In 1999, he joined Brookfield Properties as Manager, Security Systems for the Alberta region. Colin has overseen many large security projects from control center design and construction to enterprise scale card access design and installation.

Matthew Bietsch, CPO

Matthew Bietsch is a police officer in Chambersburg, Pennsylvania. He is a recent graduate of York College of Pennsylvania, where he worked in a supervisory capacity for the College's Department of Public Safety. Matt is also experienced as an adult probation officer. Matt and his brother Tim have represented IFPO at ASIS International seminars. Mr. Bietsch is a Certified Protection Officer (CPO).

David A. Black, CPP

David A. Black is a vice president with King-Reed and Associates, Canada's largest investigation agency. For the last 2 years, Mr. Black has been serving as the president of the Council of Private Investigators of Ontario. Mr. Black earned the designation of Certified Protection Professional by ASIS International and the status of Certified International Investigator through the Council of International Investigators.

Before joining King-Reed and Associates, Mr. Black was a Municipal Police Officer in Ontario Canada for 14 years, specializing in narcotics investigations and underwater search and recovery. Mr. Black began his security career in the Canadian Armed forces serving as a Military Police Officer.

In the last 10 years, much of his time has been focused on assisting corporate, institutional, and government clients with difficult terminations, incidents, and threats of workplace violence. Frequently, Mr. Black is called on to speak or provide training to groups such as Human Resources Professionals concerned with workplace violence.

John T. Brobst, Jr., CSSM, CPO

John is a security officer at Pottsville Hospital, Pottsville, Pennsylvania. He also serves as the Director of Crisis Intervention at Pottsville Hospital. He is employed as an associate director of the Paladin Security Group, a Pennsylvania consulting service. John has extensive experience in healthcare security and instructs in Nonviolent Crisis Intervention. He holds the titles of Certified Protection Officer (CPO), Certified in Security Supervision and Management (CSSM), and Certified Healthcare Security Officers.

Megan Bupp

Megan Rebecca Bupp is a May 2007 graduate of York College of Pennsylvania, where she majored in professional writing with a minor in criminal justice. Megan served as a writing tutor and made the Dean's List for almost her entire college career. Ms. Bupp has also worked as a freelance writer for *The York Dispatch*.

Tom M. Conley, M.A., B.Sc., B.A., CPP, CFE, CPO

Tom M. Conley is the President and CEO of Conley Security Agency /PSG, which is headquartered in Des Moines, Iowa.

Mr. Conley has earned and been designated a Certified Protection Professional (CPP), by the American Society for Industrial Security, has earned and been designated a Certified Fraud Examiner (CFE) by the Association of Certified Fraud Examiners, and has earned and been designated a Certified Protection Officer (CPO) by the International Foundation for Protection Officers. He is a former police captain and is a commissioned officer in the US Naval Reserve, where he possesses a secret security clearance.

Mr. Conley has earned a master of arts degree in Business Leadership with an emphasis in Quality Management from Upper Iowa University, where he graduated with a 4.0 GPA. He earned two undergraduate degrees from Upper Iowa University, a bachelor of science degree in Business Management and a bachelor of arts degree in Psychology from Upper Iowa University. He graduated with honors from both degree programs. He is also a graduate of Executive Security International, a highly regarded executive protection academy, where he became certified as a protective agent. He is a Certified Emergency Medical Technician, has earned a bona fide black belt in karate, and is a certified expert with the handgun and rifle.

Michael Dannecker, CSSM, CPO

Michael Dannecker is a sergeant with the New York City Police Department. He holds a master's degree from Marist College in Public Administration and a bachelor's in criminal justice from York College of Pennsylvania. While in college, Mike worked in a supervisory capacity with Campus Security Department as well as being a Seasonal Police Officer in Rehobeth Beach, Delaware. Mike has taken a leading role in the York College Criminal Justice Alumni Association. He is both a Certified Protection Officer (CPO) and is Certified in Security Supervision and Management (CSSM).

Mary Lynn Garcia, M.S., CPP

Mary Lynn Garcia received a B.A. in biology from the State University of New York at Oswego. She also holds an M.S. in biomedical sciences from the University of New Mexico and a Certificate in Electronics Technology from the Albuquerque Technical-Vocational Institute in New Mexico. Her previous employment has been with the University of New Mexico, Sperry Flight Systems (now Honeywell Defense Avionics Systems), and Intel Corporation. Ms. Garcia has worked for the past 13 years at Sandia National Laboratories in international safeguards and physical security. Her past projects include development of an automated video review station, video and lighting design for a demonstration physical security system at a major US airport, and project management of an integrated alarm communication and display system. She is currently teaching a series of courses at three US universities to initiate new programs in security engineering. Ms. Garcia has been a Certified Protection Professional since November 1, 1997.

Ms. Garcia has given presentations at many professional conferences including the Institute for Nuclear Materials Management, the American Defense Preparedness Association, and the American Society for Industrial Security. She has also taught several classes in security system design and evaluation within the DOE complex, to government agencies and corrections personnel, and to foreign students participating in the International Training Course jointly sponsored by the Department of Energy, Department of State, and the International Atomic Energy Agency.

Eric L. Garwood, CSSM, CPO

Eric is Security Advisor, Corporate Security, DuPont, Wilmington, Delaware. He is responsible for security at two DuPont facilities. He has served with DuPont for seven years and has been deeply involved in a major installation of card access and CCTV systems at DuPont Experimental Stations. Prior to his career in security, Eric served with the Delaware State Prison System for five years. He is a Certified Protection Officer (CPO) and a Certified in Security Supervision and Management (CSSM).

Brion P. Gilbride, CSSM, CPO

Mr. Gilbride is employed by US Customs & Border Protection, under the US Department of Homeland Security, and specializes in Intelligence Analysis and Counterterrorism Response. Prior to his government career, he worked as a first-line supervisor in both the campus security and industrial security settings. He was previously published twice in *Security Supervision: Theory and Practice of Asset Protection* and in the ASIS magazine *Security Management*. He holds a bachelor's degree in criminal justice from York College of Pennsylvania and a Graduate Certificate in Terrorism Studies from American Public University. He is currently working toward a master's degree in strategic intelligence. He is both a Certified Protection Officer (CPO) and Certified in Security Supervision and Management (CSSM).

Dr. Martin Gill

Martin Gill is Director of Perpetuity Research and Consultancy International (PRCI), a spinout company from the University of Leicester where he is a professor of criminology. The company specializes in the areas of security management, risk management, crime, and crime prevention. Martin has been actively involved in a range of studies relating to different aspects of business crime including the causes of false burglar alarms, why fraudsters steal, the effectiveness of CCTV, the effectiveness of security guards, how companies protect their brand image, the generators of illicit markets and stolen goods, to name but a few. He has published widely (12 books and over 100 articles) including *Managing Security*, *CCTV*, and the *Handbook of Security*. Professor Gill is a fellow of The Security Institute, a member of the Company of Security Professionals (and a Freeman of the City of London), he is Chair of the ASIS Research Council and an overseas representative on the ASIS International Academic Programs Committee.

Mark Gleckman, M.S., CPO

Mark is the owner of Security Management Services, Acton, California. He is a Crime Prevention Consultant and serves in that capacity for the San Fernando Police Department. He is a Technical Reserve Crime Prevention Specialist for the Los Angeles Police Department. Mark holds a master of science degree in security administration. He has

completed the Department of Defense Security Institute's curriculum in Industrial Security Management. He is a Certified Protection Officer (CPO).

Whitney D. Gunter, M.S., CPO

Whitney D. Gunter is a graduate of York College of Pennsylvania with a B.S. in criminal justice and Shippensburg University with an M.S. in administration of justice. Mr. Gunter is currently a Ph.D. student in the criminology program at the University of Delaware where he is employed as a research assistant. He is a Certified Protection Officer (CPO) and currently serves as managing editor for the International Foundation for Protection Officer's Article Archives. Mr. Gunter is a student member of ASIS International, the International Foundation for Protection Officers, the American Society of Criminology, the Pennsylvania Association of Criminal Justice Educators, and Alpha Phi Sigma.

Martin Hershkowitz, COL (MDDF-Ret)

Martin Hershkowitz, OCP, served in the Maryland Defense Force with assignment as special advisor to the commanding general. He is currently the editor of the State of Defense Force (SDF) Publication Center, producing both the SDF Journal and the SDF Monograph Series, and is a member of the Executive Council of the Military Emergency Management Specialist (MEMS) Academy sponsored by the State Guard Association of the United States, from which he was awarded the Master MEMS Badge. Within and for the US Government, Colonel Hershkowitz has served for 17 years as a Senior Security Officer for Nonproliferation and National Security concerned with the safeguards and security of nuclear weapons and the mitigation of the "insider threat": as an OPSEC (OPerations SECurity) Certified Professional; and for an additional 30+ years in military weapons analysis, educational research and evaluation, and management improvement. He is also Executive Consultant for Hershkowitz Associates and published extensively on State Defense Force Missions, critical site security and training. He is also a Certified Master Facilitator and a Certified Safeguards and Security Instructor. Colonel Hershkowitz served as ad hoc advisor to the Delaware National Guard Command Coordinator for establishing a Delaware State Defense Force.

Christopher A. Hertig, CPP, CPOI

Chris Hertig is on the faculty of York College of Pennsylvania, where he teaches courses in security management, criminal investigation, and ethics. He has also taught several physical education courses. Prior to coming to York, Mr. Hertig was a training administrator in the nuclear industry where he developed and taught various classes for both line officers and supervisory personnel.

He was a security supervisor for several years and is experienced at shopping center, college, and nuclear security. He also worked a summer as a park policeman and has done some

private investigative work. Mr. Hertig holds an M.A. in criminology from Indiana University of Pennsylvania and has completed postmasters coursework in adult education at Penn State University. The author of *Avoiding Pitfalls in the Training Process* (International Foundation for Protection Officers) as well as numerous other publications, he is active in both writing and consulting. He has been active with the Academic Programs Council of ASIS International as well as serving as a participant to the ASIS International Academic-Practitioner Symposium. He is a Certified Protection Professional (CPP), a Certified Protection Officer Instructor (CPOI), and has held instructor credentials in various defensive tactics systems. Mr. Hertig was designated a Master Level Instructor in Nonviolent Crisis Intervention.

David W. Hill, CPO, EMCA

Dave is presently employed at Williams Operating Corporation, Marathon, Ontario. He is the training officer within the Security Department and is responsible for on-site training in both Security and EMS. Dave is involved in the Occupational Health Department in which he instructs first aid and CPR programs to company employees. He has worked air and land ambulance in the Ottawa Valley and city ambulance in Sault Ste. Marie. Dave is a Certified Protection Officer (CPO).

Christopher Innace, CPO

Chris is a plainclothes anticrime officer with the New York Police Department. He is a graduate of York College of Pennsylvania and a Certified Protection Officer (CPO). He is experienced in special event security with a contract service firm as well as Retail Loss Prevention.

Glen Kitteringham, MS, CPP, CSSM, CPO

Glen Kitteringham has worked in the security industry since 1990 as a uniformed security officer, loss prevention, and insurance fraud investigator. He has worked for Brookfield Properties since 1997 and he is currently the senior manager of Security & Life Safety overseeing over 9 million square feet of commercial high-rise properties in Calgary and Edmonton, Alberta. He earned his Certified Protection Officer and Certified in Security Supervision and Management (CSSM) designations through IFPO. He is also a Certified Protection Professional through ASIS International. He obtained his masters of science postgraduate degree from the University of Leicester in the United Kingdom in 2001. He is a member of ASIS International, BOMA (Building Owners and Managers Association) Canada, IFPO (International Foundation for Protection Officers), and NFPA (National Fire Protection Association).

Bryan Kling, CPO

Bryan Kling is a Director of Loss Prevention for a mid-sized retail firm. He is a doctoral candidate in Organizational Development with Benedictine University in Illinois and has

held managerial positions in contract security. Mr. Kling also worked in private investigation while an undergraduate at York College of Pennsylvania. He is a Certified Protection Officer and has been a delegate to the ASIS International Academic-Practitioner Symposium for the past several years.

Johnny R. May, M.S., CPP, CPO

Johnny is currently employed by Henry Ford Community College (Dearborn, Michigan), where he serves as a security supervisor/crime prevention specialist with the college's campus safety department, and as the program coordinator for HFCC's Security and Private Investigations Program. He is also a licensed private investigator and adjunct professor at the University of Detroit-Mercy, where he teaches graduate level Security Administration courses. Johnny has had articles published in various security publications. He is a graduate of the University of Detroit-Mercy, where he earned his B.S. in criminal justice and his M.S. in Security Administration.

Michael McGough, D.Ed.

Michael McGough is a professor in the education department at York College of Pennsylvania. Mike is a retired school superintendent who began his career by teaching History and English. He is originally from Johnstown, Pennsylvania and has written several books on the Johnstown Flood. Dr. McGough has also developed and taught seminars on leadership.

Robert Metscher, MBA, CPP, CFE, CISSP, CSSM, CPO

Robert Metscher is the CSO for Tacoma Goodwill Industries in Tacoma, Washington. Mr. Metscher has extensive managerial experience in retail loss prevention, cash-in-transit, protective intelligence and protective program development. He served in the United States Army as a scout and has completed the Nine Lives Associates Personal Protection Specialist program. Rob co-authored "Intelligence As An Investigative Function" on the IFPO Article Archives as part of the Crime and Loss Investigation Program. Mr. Metscher holds a Masters in Business Administration as well as being a Certified Information Systems Security Professional, a Certified Fraud Examiner and a Certified Protection Professional. He is an active proponent of the "Discipline of Training" through his writing, assisting local ASIS chapters with CPP review sessions and serving on the International Foundation for Protection Officers Board of Directors.

Ronald R. Minion M.S., CPP, CPO

Ron began his career as a police officer at the age of 18 and after 8 years of law enforcement service, he founded and owned a large, well-known contract security company. He played a key role in developing the International Foundation for Protection Officers

(IFPO) and the Certified Protection Officer (CPO) program. He was one of the first examined Certified Protection Professionals (CPP). He is a graduate of Mount Royal College and earned his master's degree through Columbia Pacific University. He is a former Chapter Chairman and a longtime supporter of the ASIS International organization. In 1988, he was named International Vice President for his outstanding contributions to ASIS International.

Cole Morris, MPA, CSSM

Cole Morris is a consultant specializing in training and staff development. Widely published, his work has appeared in such publications as *Security Management, and Security Product News*. He has served as the security manager for two high-technology firms and has supervised several high-profile firms, as an adjunct instructor for a major university and also oversees security operations for a growing Phoenix-area hospital.

David H. Naisby, Jr.

David H. Naisby, Jr. is the Executive Director for the Commonwealth of Pennsylvania Justice Network (JNET), Pennsylvania's primary public safety and criminal justice information broker. Administrated by the Governor of Pennsylvania, JNET's integrated justice portal provides a common online environment where authorized users access public safety and criminal justice information. This critical information, from various contributing municipal, county, state, and federal agencies, is delivered through a secure web-based portal to over 30,000 practitioners throughout the Commonwealth's 67 counties, federal, and state agencies.

Prior to joining JNET, Mr. Naisby worked as a Parole Officer in South-Central Pennsylvania. Mr. Naisby is a published author on private security resource management. He is an alumnus of the National Criminal Justice Honor Society, the National Honor Fraternity, and he holds a B.S. in criminal justice from York College of Pennsylvania.

Brion K. O'Dell, CPP, CSSM

Brion began his career as a contract security officer in 1981 in the greater Chicago area. As he gained experience and seniority, he had the opportunity to develop emergency preparedness procedures. He was instrumental in designing security officer drills, which focused on real workplace emergencies. In 1984, Brion joined the Waukegan Port District, Waukegan Harbor, Illinois, as Chief of Security, creating the District's first security police operation, the Waukegan Harbor Patrol. In 1994, he was appointed to the position of Chief of Security, Hotel Asheville in North Carolina.

Patricia A. O'Donoghue, CSSM, CPO

Tricia is the Training Consultant for the Corporate Security Department at John Hancock Mutual Life Insurance Company in Boston, Massachusetts. She is responsible for the

coordination and implementation of training activities for all of the members of the company's protective services. She is coeditor of the security department's monthly newsletter, the *Security Post*. Tricia is a Certified Protection Officer (CPO) and has completed the Certified in Security Supervision and Management (CSSM).

Ivan E. Pollock, CSSM, CPO

Ivan is a Security Supervisor, Avenor Forest Products, Dryden, Ontario. He began his career in security with Avenor in 1981 and supervises members of the company's in-house guard force. He has completed specialized training in Non-Violent Crisis Intervention. Ivan is a Certified First Aid and CPR Instructor/Trainer. He is responsible for training members of the company guard force in life safety. He is a Certified Protection Officer (CPO) and a Certified in Security Supervision and Management (CSSM).

Ramdayal K. Ramdeen, CSSM, CPO

Kelvin is a senior security training officer for the National Maintenance Training Company Limited, Trinidad, WI, where he has served as a field supervisor and training officer for 17 years. In his current position, he is responsible for the coordination of classroom and OJT courses for a 1,300-officer security force. Kelvin is an active reserve police officer with Trinidad and Tobago Police Service. He is a Certified Protection Officer (CPO) and is Certified in Security Supervision and Management (CSSM).

Benn H. Ramnarine, MA, CSSM, CPO

Benn is the security training officer with the National Maintenance Training Security Company Limited, Mount Hope, Trinidad, WI. He is responsible for the coordination, design, development, and implementation of security training programs on a national basis. Benn is a graduate of Norwich University (Military College of Vermont). He is a member of IFPO, IALEFI, FSTMA, and MESA.

David L. Ray, B.A., LL.B

Dave is a private corporate security consultant, Calgary, Alberta. He had spent 10 years as Manager Corporate Security for Shell Canada Limited. Prior to that, he held the position of Director, Corporate Security with MacMillan Bloedel Limited. Before his work in the public sector, Dave had spent 14 years in the Royal Canadian Mounted Police. He instructs security administration and security law at the university level. Dave holds a bachelor of arts from York University and bachelor of law from Osgoode Hall Law School.

Randy J. Rice, CSSM, CPO

Randy J. Rice, CSSM, CPO, currently works as the Mail Services Coordinator for York College of Pennsylvania and is a supervisor/training officer for a local mall. Rice has

experience in retail security, mall security, hospital security, hotel security, and VIP protection. He has a B.S. from York College of Pennsylvania in criminal justice with a major in law enforcement and a minor in security. He is active in several regional mail associations across the United States and frequently writes and speaks on mail security issues. He is also an associate member of the Fraternal Order of Police and The Law Enforcement Alliance Association.

Guy A. Rossi

Guy A. Rossi is a retired sergeant with the Rochester, New York, Police Department. Sgt. Rossi's last assignment was in charge of the Recruit and Field Training Unit. He has over 21 years of experience as a street cop and trainer. His certifications include many descriptions of defense tactic and firearms training as an instructor/trainer. He is one of the founding members of the American Society of Law Enforcement Trainers (ASLET).

Randy W. Rowett, CSSM, CPO

Randy is an Assistant Security Manager with Captain Development Ltd., Toronto, Ontario. He was previously employed with the Metropolitan Toronto Police as a Special Constable, Court Detail. He has worked in hotel and harbor security and served as a private investigator and consultant. He conducts seminars for law and security students at two Ontario business colleges. He is a Certified Protection Officer (CPO) and a Certified in Security Supervision and Management (CSSM).

Henry C. Ruiz, CPP, CFE, CPO

Henry is a security specialist for a major biotechnology company. He is involved in various areas of security and related areas including training management, crime prevention research, and high-technology aspects of security operations. In addition to being a member of the IFPO, Henry is a longtime member of ASIS and the Association of Certified Fraud Examiners. He holds the CPO, CPP, and Certified Fraud Examiner (CFE) professional accreditations.

Steven R. Ruley, J.D., CPP, CFE, CSSM, CPO

Steve has more than 30 years of experience with the Walla Walla Police Department, having served in communications, records, property and evidence, and investigations. He is currently the Technical Services Supervisor with responsibilities for major crime scene investigations, forensic services, and records management. He also has more than two decades of experience in the field of security consulting. He holds a juris doctorate degree, an M.S. degree in administration, a B.S. degree in psychology and biology, and an A.S. degree in paralegal science.

Inge Sebyan Black, CPP, CFE, CPO

Inge Sebyan Black is a Branch Manager for Securitas Security Services, USA, Inc., Minneapolis, MN.

Ms. Black earned a Certified Protection Professional (CPP) certification from the American Society for Industrial Security International (ASIS) and a Certified Fraud Examiner (CFE), certification from the Association of Certified Fraud Examiners. She also earned a Certified Protection Officer (CPO) certification from the International Foundation for Protection Officers. Ms. Black was awarded the Professional Certification of Achievement from the State of Minnesota and the Federal Emergency Management Agency (FEMA) for her work in Emergency Management. In August 2001, Ms. Black successfully completed the WMD (Weapons of Mass Destruction) Incident Command (COBRA) training through the Department of Justice.

Before joining Securitas Security Services USA, Inc., Ms. Black worked in Corporate Security for several major corporations. She began her career supervising airport security in 1977. This was followed by employment as Security Administrator for National Car Rental. She also held the position of Sr. Loss Prevention Manager for JC Penney Corporation as well as specializing for many years in both physical security and contract guard security.

Ms. Black authored the section on Domestic Violence in Loss Prevention and Crime Prevention, third and fourth editions. She has served on President Reagan's Rape and Violent Crime Committee.

Jeffrey A. Slotnick CSM, PSP

Jeffrey A. Slotnick is the President of Setracon Inc. a Veteran Owned Business providing Consulting, Investigative, Protective, and Training Services for the Corporate Security, Law Enforcement, and Military communities both nationally and internationally. Setracon Inc. is headquartered in Tacoma, Washington.

Jeff is an Executive Protection Professional having graduated from R.L. Oatman and Associates course. Additionally Jeff is an Inaugural Certified Physical Security Professional and supports ASIS International in numerous capacities including Assistant Regional Vice President for Region 1a, Certifications, Guidelines, and Standards Chair for the Physical Security Council, Physical Security Professional Review Course Faculty, a member of the Private Security Services Council, and a requested speaker at numerous ASIS Events. Jeff has published articles for Tony Scotti Driving Schools, American City and County Magazine, and Security Director Magazine.

Jeff is a serving Command Sergeant Major in the Washington State Military Department where he was recently awarded the Master Military Emergency Management Specialist Badge. He is a Reserve Law Enforcement Officer for the City of Centralia, and currently possesses an active Secret Clearance. Jeff is an Army Master Trainer, Riot and Crowd Control Trainer, Taser Master Trainer, Oleo Capsicum Resin Spray Master Trainer, and Firearms Master Trainer. Jeff is an adjunct instructor for the Washington State Criminal Justice Training Commission conducting Firearms Instructor Courses and Reserve Law Enforcement Academies.

Sean R. Smith, CPO

Sean Smith is employed as a dispatcher at Princeton University. Sean worked in campus security and completed an internship with the United States Postal Inspection Service while a student at York College of Pennsylvania. He also received Behavioral Science Department Honors. He is a Certified Protection Officer (CPO). Mr. Smith has also completed the Crime and Loss Investigation Program and the Security Supervision and Management Program through the International Foundation for Protection Officers.

Todd Staub

Todd Staub, CPO (Cand.), is a 2003 graduate from York College of Pennsylvania. Todd is currently working for Bowling Brook Preparatory School as an Overnight Security Officer. He has had experience in shopping center security and served internship with a sheriff's department while an undergraduate. Todd received an Honorable Mention in the ASIS International 2002 International Student Paper Competition for his work entitled *The Contemporary Casino*. He is a member of the National Criminal Justice Honors Society (Alpha Phi Sigma) and is a candidate for designation as a Certified Protection Officer.

Charles T. Thibodeau, M.Ed., CPP, CSSM, CPO

Chuck is a prominent Minnesota College Instructor, expert witness, and security consultant. He is currently the owner of Charles T. Thibodeau and Associates in Anoka, Minnesota. Chuck has a masters of education degree, a bachelor's degree in psychology, and numerous professional certifications. Chuck has been a CPP for over 25 years. He has also served on the IFPO Board of Directors and is a past chairman of the Board. He has served in numerous executive capacities in ASIS International as well, including Chairman of the Board of the Minnesota Chapter of ASIS International.

Franklin R. Timmons, CPP, CPOI, CIPM

Mr. Timmons is currently Director of Seventrees Site Protection & Advisory Services. He and his staff provide protective and emergency preparedness strategies for several Fortune 250 companies. They were the recipients of Kimberly-Clark Corporation Dennis A. Noggle Award for service excellence in 2005.

Mr. Timmons has a bachelor of science degree from The Pennsylvania State University with a combined law enforcement, security, and training career that spans 35 years. He is a Certified Protection Professional, a Certified Protection Officer Instructor, and a Certified Institutional Protection Manager. Frank was a municipal police instructor in the Commonwealth of Pennsylvania. He is a frequent presenter at national and regional conferences.

Neal E. Trautman, M.S., PhD

Dr. Trautman is the founder and director of the nonprofit National Institute of Ethics, where he is responsible for all aspects of ethics-related services. He is the founder of the Law Enforcement Television Network (LETN), the nation's largest provider of law enforcement training, serving more than 120,000 officers. During Neal's 16 years as a sworn officer, he has received many prestigious awards including two decorations for heroism. He has authored eight textbooks and is the founder of the nationally recognized Florida Criminal Justice Trainer's Association.

Christopher L. Vail, M.S.

Chris is the president of Law Enforcement Development, a firm specializing in training security and law enforcement personnel in such topics as first-line supervision, testifying in court, and investigative techniques. Mr. Vail began his career as a military policeman with the US Marine Corp. His security experience includes being in charge of security for a high-profile Congressional Committee. He has also served as Director of Security on a college campus. Mr. Vail has served as president of the Georgia Criminal Justice Educator's Association. Chris is also presently the executive director of the Police Supervisors Group.

Ernest G. Vendrell, Ph.D., CEM, CPP, CPO

Ernest Vendrell is an assistant professor, as well as the Chair of Emergency Management Programs, at Lynn University, situated in Boca Raton, Florida. He earned a Ph.D. in Public Administration and Policy, a masters in management, and a master's and bachelor's degree in criminal justice. In addition, he was awarded a Fulbright Fellowship in Police Studies with the United Kingdom in 2000, and was a visiting fellow at the University of Leicester, Scarman Centre for the Study of Public Order. His research project was entitled "Preparing for the New Millennium: A Comparative Analysis of Emergency/Disaster Management Professional Development Strategies for the Police Service."

Dr. Vendrell retired from the Miami-Dade Police Department in 2002 after 27 years of sworn law enforcement service. Throughout his career, he worked in a variety of patrol, investigative, supervisory, and administrative capacities. In particular, as a training supervisor, he was responsible for providing training in Critical Incident Management to many police officers and governmental officials from the South Florida area.

Dr. Vendrell is a Certified Emergency Manager (CEM), a Certified Protection Officer (CPO), as well as a Certified Protection Professional (CPP). He is also a member of ASIS International, where he serves on the Crisis Management and Business Continuity Council.

Mavis Vet, CSSM, CPO

Mavis has been employed by Llewellyn Security Group since 1986 as a security supervisor. She has completed the private investigator's program through the International School of Investigations and Protective Services. She has also achieved special protective service training in narcotic and explosive detection techniques and leadership training in behavior symptom analysis. She is a Certified Protection Officer (CPO) and a Certified in Security Supervision and Management (CSSM).

Scott A. Watson, MCJ, M.Ed., CPP, CFE

Scott Watson is a consultant, author, and teacher, specializing in the areas of organizational security, crisis management, and educational services. He holds a bachelor of arts degree in political science from Long Island University, a masters of criminal justice administration from Boston University, and a masters of education from the University of Massachusetts.

Mr. Watson is a Certified Protection Professional, a Certified Fraud Examiner, and a frequent speaker at professional conferences. He currently teaches security management at Boston University's Center for Professional Education and has previously taught online courses in Emergency Planning, Disaster Theory, and Workplace Violence for American Military University.

Mr. Watson is a member of ASIS International, where he serves as the vice chairman of Crisis Management and Business Continuity Council. He also serves on the ASIS School Violence Task Force and is a member of The Association of Certified Fraud Examiners and the New England Disaster Recovery Information Exchange.

R. Gene Watson, CSSM, CPO

Gene is Protection/Investigation Chief for Bank IV Oklahoma, Tulsa, Oklahoma. He is a retired police officer and Town Marshall. He is considered an expert in financial security and emergency security management. Gene is a certified instructor in private security and private investigations in Oklahoma. His professional training includes completion of the FBI specialized protection training courses. His security policy manuals have been published by several financial institutions.

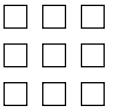
Eric Webb

Eric Webb is the Deployment Coordinator for the Pennsylvania Justice Network. Eric works with a team of developers, trainers, and business analyst to identify and meet the information needs of criminal justice professionals in the Commonwealth of Pennsylvania. Formerly, he was an assistant supervisor with the York County Adult Probation Department where he was responsible for mentoring and training new officers. Mr. Webb graduated cum laude from York College of Pennsylvania with a dual major in security and sociology.

Jimmy Wilson, CPOI, CPO

Jimmy Wilson is currently the Director of Security/Safety for Arizona Charlie's Hotel & Casino. During his 26 years in the security field, he initiated the first Security Bike Patrol on a strip property and has opened both MGM Grand and The Stratosphere Hotel and Casino, located in Las Vegas, NV. While at The Stratosphere, he worked hand-in-hand with the Las Vegas Fire Department in the development of planning and organizing safety and security measures for the opening of the Stratosphere Tower. Jimmy is best known for promoting professionalism through the implementation of the Certified Protection Officer program.

This page intentionally left blank



Dedication

To the most remarkable man I know …. Mr. Ron Minion. Not only did Ron serve as my MENTOR in the security industry but in my life as well. Knowing him and the qualities he possess has been the greatest gift. I treasure every moment shared with him.

Ron's vast knowledge of the security industry and his enthusiasm and commitment to professional development have created a path for us all to follow.

YOUR GREATEST FAN—*Sandi J. Davies*

We had spoken and corresponded numerous times before meeting in person. As I recall, it was 1983 at a meeting in Chicago. We talked and drank beer at the hospitality suite.

The next morning I went down to your room to pester you. You were shaving and took my harassment good naturedly.

Over the next two decades, I pestered you continuously. You would cheerfully acknowledge your young friend and we would work together. Our goal was to educate, train, and recognize security officers. The means of this effort included articles, books, programs, certifications, and professional organizations. You were the epicenter: juggling tasks between running a security company and training dogs. But I know that protection officers were your first love.

Damn few people have given as much of their money, time, and energy to what they believe in as you have.

Those of us who are privileged to know you will always be grateful. We must pass along the gifts you gave to those not fortunate enough to have made your acquaintance.

Those are our marching orders.

Christopher A. Hertig, CPP, CPOI
Behavioral Sciences Department
York College of Pennsylvania

Mentor, Hero, & Dad …. You have been all of these to me Ron Minion. As a child, I watched you build a security company from the ground up. Working the night shift at ATCO Industry just you and your four legged companion to keep you company. By day you would hustle to get new clients and do the necessary administrative work.

Since the beginning, you wanted to bring professionalism to the industry. So it was no big surprise that you implemented training programs to enhance your guards as you built your business up. You were innovative and a leader in professionalizing the security industry. You coined the expression "Knowledge to Protect" and it became your logo.

You are a remarkable man and I not only had the honor of working beside you in the Security Industry but also to have you as a father. Thank you for all you taught me and the thousands of others in the Security Industry.

Your Loving Daughter—*Heather L. Minion*

Dad,

Since a little boy you have always taught me the importance of honor, respect, and discipline. Honor in self and family, respect in yourself and for others, and discipline in uniform and career.

I cannot thank you enough for teaching me some of the valuable lessons and character traits that have made me the Soldier I am today. I love you Dad.

Specialist Leroy D. Minion
101st Airborne
Ft. Campbell, KY

Foreword

Louis A. Tyska and
Lawrence J. Fennelly

This is, in our opinion, a one-of-a-kind text that has been specifically written and offered to readers: the Supervisor or Manager; the aspiring protection officer or university student. There is no substitute for experience but this goes a long way in preparing the readers (participants) for their journey on the management career path. When we were both supervisors, there was no text and very little additional training provided for supervisors. We salute all of the many contributors who assisted in putting the text together and sharing their expertise to make the path easier to attain supervisory skills and abilities.

During the past five years, a lot has changed both nationally and internationally. Homeland Security has developed and terrorism remains an everevolving threat. Organized retail crime, identity theft/information loss, and natural disasters also continue to be major concerns of protection professionals.

Consequently, the education and training provided must meet these threats. Supervisors and managers must be well versed in these topics and must inspire their subordinates to acquire more education, training, and experience. They must continually emphasize professional growth and development of the individual officer, agent, or investigator.

Organizational development occurs when substantial numbers of the protection organization have undergone professional development experiences.

Programs offered by the International Foundation for Protection Officers and our allied organizations are examples of professional growth experiences. Individual employers and colleges may create their own.

Regardless of origin, the supervisor is the conduit for professional growth. He or she must embrace opportunities for professional and organizational development. He or she must lead by example.

What Is a Supervisor?

- The person who represents higher authority.
- The person who assesses situations and conditions to make on-the-spot judgments without favor, prejudice, or fear.
- The person who is a responder to any and all situations.

- The person who must galvanize the efforts of many to attain stated goals.
- The person who must assign tasks and ensure compliance and constant quality performance.
- The person who is accountable and, therefore, first in line to shoulder reaction, both good and bad.
- Finally, the person who must make a decision for management based on his or her professional development.

What does it mean to be a supervisor? First, they may be called on to handle numerous conflicts. Second, they will be required to meet management's or their client's expectations in the daily routine of operational activities.

The supervisor is the backbone of the organization. His/her scope of responsibility is rather unique.

What Is a Manager?

- A manager designs and develops security, safety, and investigative programs.
- Managers work with budgets and other resources (equipment, uniforms, technology, software, etc) to ensure that the protective mission is achieved.
- Managers oversee processes (procedures) that accomplish organizational goals and objectives.
- Staff functions without a supervisory span of control over line employees may be performed by managers. Training, technical support, auditing, etc. are staff functions.
- A manager coordinates activities rather than supervises them.
- A manager is charged with policy formulation.
- Managers oversee line supervisors such as shift leaders, sergeants, lead officers, etc.
- Managers interact with department heads and upper management (president, vice president, chief financial officer, chief, director, etc.)

Professional Development

Professional development is a critical concept. It is the pathway for supervisors to *become* managers. By professional development we are referring to:

- Leadership and networking skills.
- Communicative ability that includes, oral, written, and computer skills.
- Reasoning and logical thinking ability.
- Receiving formal training, accreditation, or certification for one's professional growth and personal satisfaction.
- Developing a personal and professional code of ethics and high standards by which to guide oneself.
- Mentoring and coaching through on-the-job training and in-house programs.

- Turnover and job rotation can create overall improvement *and* a challenge.
- Staying current on industry events by reviewing news sources, trade publications, and web sources such as the IFPO Article Archive among others.

As the job changes, so must the training and the level of skills within the department increase. Professionals develop a "discipline of training" and continuously seek to improve their knowledge and abilities.

New Supervisors/Managers

The most demanding problem for the supervisors within a protection department will be the transition from the position of security officer to that of supervisor. The supervisor's role should be to assist in enabling the manager to provide a level of support within the organization. Supervisors must take responsibility for corporate regulations, moral and ethical tone as well as providing the required level of security and customer service required.

Similarly, new managers have some adjusting to do. We feel it is important to advise readers that as a new manager, one has to learn how to develop and exercise (not abuse) their newly acquired authority, power and influence effectively. This can be done by establishing one's credibility—the earning of subordinate's commitment and support.

Management is an art as well as a science; it is, perhaps, more art than science. New managers are at the crossroads, looking to make the right turns. Consider the following: A new manager is the person in charge. His/her elevation to the status of manager through promotion has given him/her the authority.

- A new manager is a person with a level of power and is a decision maker.
- A new manager is knowledgeable in his/her field.
- A new manager uses his developed skills, ideas, education, and experience.
- A new manager supervises his subordinates and passes information down the line as well as up the chain of command.
- A new manager has the responsibility to be aware of employer policy as well as client requirements and the level of security required within the organization.

As one develops his on-the-job experience as a new manager, he starts to understand and accept the new responsibilities as well as what it means to be a manager.

Those who have been promoted to the rank of supervisor or manager should:

- Learn how to supervise and adjust to the new role.
- Develop leadership skills.
- Develop interpersonal skills.
- Develop knowledge of who they are. *Know thyself.*
- Learn how to cope and deal with stress and emotion associated with management concerns.

As one progresses in his/her career, these learning points become ingrained. They become second nature. They become part of oneself.

Conclusion

Supervisors and managers will be called on to make decisions everyday; some will be easy; others quite difficult. Every decision cannot have been made properly without a foundation of education, training, and experience, supported by "street smarts." Decision-making ability may be introduced in a classroom or from a book; it is perfected through experience. Being on the front line and being prepared and willing to make the tough decisions is what being an effective security supervisor and manager is all about.

Acknowledgments

Compiling a book of this nature requires a tremendous amount of teamwork. Without a doubt, the team members who worked on this project put their hearts, heads, and souls behind their efforts. The result is a work that we can all take great pride in. It will long serve as a tool that enhances the security industry's body of knowledge.

The team that so unselfishly contributed to this project richly deserves recognition.

A very special thanks to each professional who contributed information in the area of his or her expertise. The time, effort, and commitment of each and every contributor is greatly appreciated.

The contributions made by these dedicated team members provide the framework of a significant undertaking that brings positive recognition to the private/public security sector. It will help those who implement and manage security to find the tools to work with, and it will help those who need protection better understand the horrendous challenges involved in keeping an organization and its people safe and secure.

Special thanks to Christopher A. Hertig, CPP, CPOI. Without his energy, direction, and dedication to the team goals, we could not have developed this purposeful reference text that will serve so many.

Other members of the team included Chuck Thibodeau, CPP, CSSM; Inge Sebyan Black, CPP, CFE, CPO; and many students of York College of Pennsylvania.

Space precludes us from individually recognizing all contributing authors, so we draw your attention to the outstanding credentials of each of the 30-plus writers.

And finally, a salute to the International Foundation for Protection Officers (IFPO) whose unselfish commitment to professionalism is evident through this notable contribution.

This page intentionally left blank

Introduction

Sandi J. Davies and
Christopher A. Hertig

Sandi J. Davies, Coeditor

Sandi began her career in contract security in 1980 with a primary focus on personnel administration. She became deeply involved in training and was instrumental in developing security officer training programs for a major national guard company. Her interest in security training grew, and in 1988 she joined the newly formed International Foundation for Protection Officers (IFPO) as an administrative assistant. In 1991, she was named executive director of the IFPO and has been a driving force in Foundation program development and administration ever since. Sandi is a longtime member of ASIS International, having served in various executive positions at the chapter level. Sandi is also a member of the ASIS International Private Security Services Council.

Christopher A. Hertig, CPP, CPOI, Coeditor

Chris began his career in 1975 as a part-time student aide in the Security Department during his junior year in college. He has worked as a security officer and supervisor in various settings. In 1980, he became a Nuclear Security Training Administrator where he developed instructional materials and taught security personnel. In late 1982, he met a young woman named Carla who inspired him to continue his graduate education and write for publication. He subsequently began writing and has published hundreds of articles, reviews, chapters, and books.

In 1984, he married Carla, completed his master's degree, and joined the Behavioral Sciences Department at York College of Pennsylvania. Chris has been active on the ASIS International Academic Programs Council. He is a member of the Board of Directors for the IFPO and has worked with the National Partnership for Careers in Law, Public Safety, Corrections, and Security. He has held instructor credentials in a number of subjects and is both a Certified Protection Professional (CPP) and Certified Protection Officer Instructor (CPOI).

Security Supervision and Management Text

Demand for the Security Supervision and Management Program, which was developed in 1990 by the International Foundation for Protection Officers (IFPO), has continued to grow. As new components were added to the program, a more current, relevant course text had to be developed. Commensurate with this demand was the need for college and university courses in security, asset protection, and emergency management. The need to provide web support for the book was also apparent.

The IFPO embarked on the task of completing a new text to fulfill these needs and engaged security professionals to contribute to this effort. The result was the forming of an alliance between the IFPO/Butterworth-Heinemann and some of the industry's leading security supervisors, authors, educators, and consultants, who collectively contributed to the production of this text.

The book for security leaders is here. It serves participants in the Security Supervision and Management Program as well as students in other IFPO programs (visit ifpo.org). *Security Supervision: Theory and Practice of Asset Protection* provides a broad foundation of knowledge, making it an ideal course text as well as a valued reference for all protection practitioners.

Security Supervision and Management Program

Objective:

To facilitate the academic and professional development of security professionals who aspire to enhance their leadership skills.

To deliver a functional supervisory/management instructional program developed to heighten each candidate's ability to master the techniques of security personnel management.

To provide a meaningful accreditation which will lend professional recognition to those candidates who exhibit the knowledge and skills required to be Certified in Security Supervision and Management (CSSM).

History of the Program

The IFPO was founded in 1988. A dedicated group of well-known senior members of the international security community set out to develop a nonprofit organization that would address the professional training and certification needs of security officers and first-line supervisors.

Through the commitment and vision of these industry leaders, who became members of the Board of Directors, the IFPO was formed. The Foundation's first and foremost undertaking was to develop the Certified Protection Officer (CPO) Program. Since the inception of the program, thousands of officers have earned their CPO accreditation, now the recognized designation for professional officers employed by proprietary and contract security forces worldwide.

As the IFPO grew, so did the need for Foundation leadership in addressing the professional development requirements of members of the security industry. Security officers earned seniority and often assumed leadership roles within their respective security organizations. The IFPO recognized that there had to be a learning progression, a better defined professional development/career path. The Board of Directors and Foundation administrators subsequently developed the Security Supervisor Program and Certified Security Supervisor (CSS) designation. In 2004, the IFPO Board of Directors elected to rename the program and it evolved into the Security Supervision and Management Program and Certified in Security Supervision and Management (CSSM). This title change better reflects the content and emphasis of the program materials.

Security Supervision and Management Program Logistics

To facilitate each reader's learning opportunities, at the conclusion of each chapter, the author has included a selection of fill-in-the-word, true/false, and multiple choice questions. To complete the Security Supervision and Management Program, each candidate must successfully achieve a score of no less than 70% on both an interim and final examination. Once the applicant has successfully completed this process, he/she would be awarded a certificate of completion for the Security Supervision and Management Program.

The candidate then may elect to proceed with the Certified in Security Supervision and Management (CSSM) Program if he/she so qualifies. Candidates enrolling into this program must have 18 months of security experience with a minimum of 6 months at the supervisory or managerial level.

The CSSM program candidates are required to select and analyze a series of workplace scenarios that describe on-the-job conditions which are frequently encountered by the working security supervisor and/or manager. Each situation demands immediate leadership action. Candidates must describe in detail the appropriate actions recommended to bring the matter to successful conclusion. The corrective measures employed by the supervisor or manager must be supported from the contents of the course text.

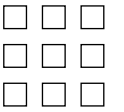
Candidates seeking the CSSM accreditation must submit an affidavit in the prescribed form, declaring that the written portion of the program is authored entirely by the applicant seeking accreditation.

The CSSM certification committee will review the scenarios and application along with the candidate's complete file to determine eligibility for the certification.

Conclusion

The Foundation has developed an important relationship with Butterworth–Heinemann (BH), who have responded positively to the need to recognize the working security professional as well as those studying asset protection in colleges and universities. Without the continued support of BH, it would be difficult for the IFPO to exercise its mandate of providing professional development opportunities to the rapidly expanding security industry.

This page intentionally left blank



Protection Officer Code of Ethics

The Protection Officer shall …

1. Respond to employer's professional needs
2. Exhibit exemplary conduct
3. Protect confidential information
4. Maintain a safe and secure workplace
5. Dress to create professionalism
6. Enforce all lawful rules and regulations
7. Encourage liaison with public officers
8. Develop good rapport within the profession
9. Strive to attain professional competence
10. Encourage high standards of officer ethics

Protection Officer Code of Ethics

Today business and the public expect a great deal from the uniformed security officer. In the past, there has been far too little attention paid to the ethical aspects of the profession. There has to be solid guidelines that each officer knows and understands. More importantly, it is essential that each manager and supervisor performs his or her duties in a manner what will reflect honesty, integrity, and professionalism.

Every training program should address the need for professional conduct on and off duty. Line officers must exhibit a willingness to gain professional competency and adhere to a strict code of ethics that must include the following.

Loyalty

To the employer, the client, and the public. The officer must have a complete and thorough understanding of all of the regulations and procedures that are necessary to protect people and assets on or in relation to the facility they are assigned to protect.

Exemplary Conduct

The officer is under constant scrutiny by everyone in work and public places. Hence, it is essential that he/she exhibits exemplary conduct at all times. Maturity and professionalism are the key words to guide all officers.

Confidentiality

Each officer is charged with the responsibility of working in the interests of his/her employer. Providing protection means that the officer will encounter confidential information which must be carefully guarded and never compromised.

Safety and Security

The foremost responsibility of all officers is to ensure that the facility must be protected; is safe and secure for all persons with lawful access. The officer must fully understand all necessary procedures to eliminate or control security and safety risks.

Deportment

Each officer must dress in an immaculate manner. Crisp, sharp, clean, and polished are the indicators that point to a professional officer that will execute his/her protection obligations in a proficient manner and will be a credit to the profession.

Law Enforcement Liaison

It is the responsibility of each officer to make every effort to encourage and enhance positive relations with members of public law enforcement. Seek assistance when a genuine need exists and offer assistance whenever possible.

Strive to Learn

To become professionally competent, each officer must constantly strive to be knowledgeable about his/her chosen career. How to protect people, assets, and information must always be a learning priority for every officer.

Develop Rapport

It is necessary to be constantly aware of the image that our profession projects. All officers can enhance the image of the industry, their employer, and themselves. Recognize and respect peers and security leaders throughout the industry.

Honesty

By virtue of the duties and responsibilities of all officers, honest behavior is absolutely essential at all times. Each officer occupies a position of trust that must not be violated. Dishonesty can never be tolerated by the security profession.

Prejudice

The job of protecting means that the officer must impose restrictions on people that frequent the security workplace. All human beings must be treated equally, with dignity and respect, regardless of color, race, religion, or political beliefs.

Self-Discipline

With the position of trust comes the responsibility to diligently protect life and property. These duties can only be discharged effectively when the officer understands the gravity of his/her position. Self discipline means trying harder and caring more.

Conclusion

The job of protecting life and property focuses much attention on the individual security officer. Hence, it is essential to be aware of the need for professional conduct at all times. By strictly adhering to each section in this code of ethics, it may be expected that we as individuals and the industry as a whole will enjoy a good reputation and gain even more acceptance from the public as well as private and government corporations. You as the individual officer must be a principal in this process.

UNIT I

Security and Asset Protection Principles

This page intentionally left blank

1 Evolving a Discipline of Security

Martin Gill[1]

Although security as a form of activity has a long history, the formal academic study of it is a much recent affair. Indeed, the discipline of security is still evolving. One paper has lamented the lack of research, the lack of academics interested in security, and the lack of PhDs on the topic,[2] and according to these criteria, the state of the security discipline is poor. Indeed, a "Special Issue" of the *Security Journal*, now the most established refereed journal in this area, was devoted to assessing the current state of security knowledge. While the papers were generally optimistic about the discipline moving forward, some lamented the fact that it had not moved very far in the previous two decades. For example, Giever[3] noted that the discipline is immature, lacks funding, and is evidenced by the lack of scientific research. Beck,[4] Gill,[5] and Grabosky[6] all highlighted the fact that many of the problems that existed in previous years, including poor quality data and the lack of economic analyses of security cases, still characterized security today.

Indeed, despite the large amount of criminological work on a variety of different types of victims, there is still very little research on offences within, by, and against organizations.[7] There are numerous very good studies on crime, crime prevention, management, and risk, but few attempts have been made to integrate the knowledge and experience being gained, not in a security context. And there has been little effort within the security sector for practitioners and academics to learn from each other. Each has worked in relative isolation, and thus there has been a lack of critical thinking on the links between theory and practice: academics are suspicious of solutions to problems whose impact has not been precisely measured, while practitioners on the other hand dislike the delay inherent in the academic process, claiming that the commercial realities demand a swift reaction. Moreover, practitioners are sometimes

---

[1] Director of Perpetuity Research and Consultancy International, a spinout from the University of Leicester, m.gill@perpetuitygroup.com.

[2] E. Borodzicz and S. Gibson (2006). Corporate security education: Towards meeting the challenge. *Security Journal* 19(3):180–195.

[3] D. Giever (2007). Security education: Past, present and the future. *Security Journal* 20(1): 23–26.

[4] A. Beck (2007). The emperor has no clothes: What future role for technology in reducing retail shrinkage? *Security Journal* 20(1):57–61.

[5] M. Gill (2007). The challenges for the security sector: Thinking about security research. *Security Journal* 20(1):27–30.

[6] P. Grabosky (2007). Security in the 21st century. *Security Journal* 20(1):9–12.

[7] Given that the interest here is in workplaces, the use of "business" is contentious. The word "organization" better reflects the fact that workplaces exist in the voluntary and public sectors. It is, however, a less familiar word in this context. In this chapter, they will both be used to denote workplaces.

confused by the mode of presentation which is weighted with jargon and generally speaking the security sector has not sought to systematically benefit from the findings of independent research. There have been few attempts to clarify the subject matter of a discipline of security. The subject has drawn considerably from criminology, while the background of criminologists is generally confined to two main disciplines: sociology and law.[8] Perhaps as a consequence, the contribution that other disciplines (e.g., history, intelligence studies, environmental science, engineering, forensic science, and in particular management and risk management) can make has only recently begun to be fully exploited,[9] and there are many more that could be. Indeed, what subject is there that cannot and does not in some way contribute to our understanding of security? For this writer the answer is "none."

Similarly, the approach of practitioners is fragmented. On a representational level, this is evidenced by the range of security associations and institutes that exist often with conflicting aims, and a common characteristic of the structure of security representation around the world is that there is no single voice that can speak for what is a diverse range of activities. If one was starting from scratch and seeking a good voice for security activities, then the structures of the security world would look very different to the way they do now. It is no wonder that those working within the security world should argue that there is a need to take steps to ensure that they are regarded as a profession, while those outside point to the lack of formalized training, and in many countries the absence of statutory regulation (or the poor status of it) as evidence that it has a long way to go.[10] In reality, both camps are right. The security world is full of dedicated and very highly skilled individuals, but the world in which they work has yet to find the right structures to ensure that minimum standards are maintained for all those practicing its skills. This remains a challenge for the future. In the meantime, works goes on, security practitioners continue to offer excellent service to their clients, associations continue to push for recognition of their members' work and form the basis on which a recognition as a profession can one day be built. Associations have been instrumental in the development of a range of very good training courses which have their own impact on raising standards.

However, I want to look at the role of universities and other research bodies, or more specifically at some of the research that has evolved in recent years which is making its own contribution to practice. The good news for the security world is that a range of universities now offer postgraduate courses. Often these are attended by professional people who are keen to obtain the academic credibility to accompany the skills they have acquired over many years. In the past, I have been intrigued by the types of comments that our students make on the successful completion of the program, such as "how come I have been a security practitioner for years and never have taken a course in crime prevention?" And I have to say "I don't know." Universities are able to develop theories, provide frameworks, and generate new ideas to guide practice. This is where universities have made a difference to the lives of security professionals and to the development of the security world on its road to a profession. And as from 2006, ASIS International has a dedicated Research Council which is committed to generating new research findings.

An academic discipline, and the study of security aspires to be just this, is dependent on knowledge. And universities and a range of research institutes and organizations are beginning to publish research to develop that knowledge. In this chapter, I would like to highlight just three areas where this is the case, where research is already appearing. They are the value of security, on policing, and on the role of management in responding to crime.

---

[8] P. Rock (1994). The social organization of British criminology. *In* "The Oxford Handbook of Criminology" (M. Maguire, R. Morgan, and R. Reiner, Eds.). Oxford: Clarendon Press.

[9] However, see M. Gill (Ed.) (2006). The *Handbook of Security*. Palgrave: Macmillan for a good discussion of a broad range of issues including the contribution of different subject areas to the study of security.

[10] See the Chapter by M. Button and B. George in the *Handbook of Security* (footnote 5). See S. Box (1983). *Power, Crime and Mystification*. London: Tavistock.

The Value of Security

It has long been recognized that businesses are offenders and that this impacts on the community.[11] Rather less has been said about the extent to which crimes committed against businesses and against workers impact on society. Workplaces are commonly victims and sometimes considerably more so and workers too are victimized at work.[12]

It needs to be stressed that crime at the workplace has a direct impact on people: organizations include employees, employers, contractors, and customers,[9] and it is right to be concerned when they are victimized, all the more so given the legal requirement on employers under health and safety legislation to provide a safe working environment.

Crime is expensive and so too are the costs of protecting against crime. At least some of the resulting costs are passed on to consumers in increased prices; and it is the poorer sections of the community who can least afford this burden. For the organization it can be expensive in other ways, resulting in high staff turnover with subsequent recruitment and retraining costs, let alone the costs that may result from the disruptions caused by people leaving and joining. There may also be an impact on the brand, this is an extremely important part of an organization's value. A reputation can be hard to earn and quick to loose, and the implications can be felt on the bottom line.

Companies sometimes suffer losses because of the illegal activities of their own staff. Sometimes this can have catastrophic consequences. Nick Leeson was a trader who worked for Barings Bank but set up an illegal account and ran up massive debts as a consequence of poor and illegal trading gambles. Eventually he fled abroad, was captured in Germany, and returned to Singapore to serve a prison sentence. The total damage suffered by Barings was $1.4 billion. In February 1995, Barings was declared bankrupt.

The costs of crime are serious, add up the costs of counterfeiting, frauds and other types of staff dishonesty, thefts, and the need to protect against crime, and it becomes a multibillion dollar industry. Yet during the period when crime has come to the forefront of public concern, security has all too often been seen as marginal to business. This is primarily due to the fact that it has established itself as an area of activity which is value adding, all too often security is seen as the poor relation of other departments such as sales, marketing, and finance, which make a positive contribution to the bottom line, all too often security is seen as a cost.

One recent study,[13] based on interviews with security practitioners in different parts of the world including Australasia, Europe, and North America, has highlighted the fact that many security practitioners accepted that they were a cost and were not aware of the potential to view security as adding financial value, yet, as this and other studies have shown, it clearly can.[14] Security needs to align itself with business's objectives, assess the risks to achieving them, and understand weaknesses and security vulnerabilities in all business processes; it needs to collect good quality and appropriate data and use all this information to "talk the language of business."[15]

Part of the problem is that there is not a discipline of security that everyone signs up to. And even if there were and practitioners sign up now they would find it lacking. In the United States, more than Europe, business studies is a part of the study of security, but it is fundamental. And if the practice of security is to be accorded a higher status, it needs to develop frameworks that can inform practice and that become essential reference points.

---

11 For different examples, see R. Smith (Ed.) (2002). *Crime in the Professions*. Aldershot: Ashgate; and S. Box (1983). *Power, Crime and Mystification*. London: Tavistock.

12 British Retail Consortium (2006). *Retail Crime Survey 2005*. London: British Retail Consortium.

13 M. Gill, A. Howell, G. Keats, and E. Taylor (2007). *Demonstrating the Value of Security*. Leicester. Perpetuity Research and Consultancy International. www.perpetuitygroup.com/publications.

14 See, Booz Allen Hamilton (2005). *Convergence of Enterprise Security Organizations*. US: The Alliance of Enterprise Security Risk Management; R. Briggs and C. Edwards (2006). *The Business of Resilience*. London: DEMOS.

15 Gill *et al.* (op cit).

But as Button has noted,[16] this will not be enough. There will need to be a change of mind-sets. Practitioners will need to embrace the learnings and for that to occur, there will need to be dissemination strategies that allow security research findings to be presented in "user-friendly" ways, and/or practitioners can be encouraged to read scholarly journals.

Policing

There is a considerable amount of research on "the police" but comparatively fewer studies focus on private policing (and fewer still on contract guarding and in-house security), although recently there have been some very good publications which in different ways have provided insights into private security sector work.[17] There have also been some very good studies of the relationship between the private sector and forms of public policing,[18] and here the important role that private security plays in policing society is given credence. Of course, on the one hand, private security unlike the public police is accountable only to those who pay, but an important function is fulfilled. And although it is not much discussed, there are a number of studies that have highlighted favorable perceptions of the work of private security personnel.[19]

But private security is provided in a variety of forms. For example, in the private and public sectors, in the voluntary sector, and informally via friends and neighbors. But even within the private sector, it can take a variety of forms. Clearly there are security companies that provide security services, sometimes companies employ security officers directly and sometimes they engage contracted security personnel to guard their premises, although they may wear the uniform of the client organization so that customers would not be aware of this. There are other variations, in the United Kingdom some train companies agreed to pay for staff to be employed by the British Transport Police (BTP, the organization responsible for policing the railways). The BTP are exclusively responsible for deployment, even though all costs are met by the train operators. And there are other links. In the United Kingdom, it is recognized in legislation that there are a range of people who could help the police and the chief of police can, if he or she wishes, accredit individuals to help provide security. They have at the most very limited powers but are invested with a duty to help the police. And volunteer police officers (they are called Special Constables in the United Kingdom), who have limited police powers, can be of help to business. Indeed some retailers have agreed that employees who are Special Constables can undertake a limited number of hours of duty as part of their employment.[20]

What this discussion hopefully shows is that there are quite a few different types of overlaps between private and public security. That private security has a number of different roles and these can be important. Indeed, no study of policing (as opposed to the "police") is complete without considering the many manifestations of the private police provision, and this too is a largely unexplored topic. And again it is another area where the discipline of

---

16 M. Button (2007). Developments in security. *Security Journal* 20(1):51–54.

17 M. Button (2007). *Security Officers and Policing*. Aldershot: Ashgate; A. Wakefield (2003). *Selling Security: The Private Policing of Public Space*. Cullompton, Devon: Willan Publishing.

18 For example, see D. Bayley and C. Shearing (2001). *The New Structure of Policing: Description, Conceptualization and Research Agenda*, Research Report NCJ 187083, Washington DC: National Institute of Justice; L. Johnston (2000). *Policing Britain: Risk, Security and Governance*. London: Routledge.

19 For example, see, A. Beck and A. Willis (1995). *Crime and Security: Managing the Risk to Safe Shopping*. Leicester: Perpetuity Press; L. Noakes (2000). Private cops on the block: A review of the role of private security in residential communities. *Policing and Society* 10:143–161; T. Prenzler and R. Sarre (2002). The policing complex. *In* "The Cambridge Handbook of Australian Criminology" (A. Graycar and P. Grabosky, Eds.), pp. 52–72. Melbourne: Cambridge University Press.

20 For fuller discussion see, M. Gill (Ed.) (2006). *Introduction, the Handbook of Security*. Palgrave: Macmillan.

security is just evolving and when it does, it may offer a range of ways in which the practice of security may be enhanced and indeed, with proper accountability structures in place, appropriately expanded.

The Role of Management – Responding to Crime

Evaluations of responses to crime, whether within an organization or in a community setting, need to take account of both technological and management factors, and not just the former. As Hayes[21] has summarized:

> *Swiftly changing technologies will greatly enhance loss control efforts, but good, sound leadership and management provide the ultimate resolution to loss control problems.*

It is interesting to note that the literature on security management (which consists more of guides and manuals than of studies) includes relatively few evaluations of management approaches. Indeed, the security world has often found solutions before defining the problems, and there is a need here for more and better evaluations. CCTV is a classic example. A major evaluation of CCTV in the United Kingdom has shown how it is frequently installed without a meaningful set of objectives; without proper risk assessments to confirm that there really is a problem in the first place and that CCTV is an appropriate solution; without an effective implementation strategy; without ensuring that management and staff are prepared for the task to name just a few points.[22]

Of course, one of the realities of crime prevention (and of management), and one of the difficulties too, is that it is sometimes more important to be seen to be doing something, anything, than to be doing the right thing. Purchasing a CCTV system is a more visible sign that safety and security are being taken seriously (especially when rivals are doing so) than minor changes in policy, such as altering operating procedures for cashiers or security staff or by focused training of staff. Yet these may be more appropriate and cheaper. It is unlikely that there will be uniform solutions even to common problems. There are too many variables that need to be taken account of, including personnel, culture, language, laws, products, markets, competitors, and finance. But there may be simpler responses that are also better. The discipline of security has lacked good management and business inputs, and the practice of security has also suffered, and herein rests an opportunity.

Toward a Body of Knowledge

So the signs are good, more research is being produced which greatly enhances the development of security into a recognized field of study, but there is a need to bring this work together to create a recognized body of knowledge, a set of theories and frameworks that can be readily identified with the security world.[23] The world of risk management, for example, has identified distinct approaches, and there are a range of areas where security can benefit from work that has been developed, for other purposes over many years, different areas of the study of management, including disaster management, organizational studies, the sociology of work, and of course crime prevention to name but a few. Indeed, within the world of crime prevention, a considerable amount of effort has been devoted to understanding how offenders make decisions at the scene, the sorts of things that make them think about the desirability of carrying out an offence in what is called rational choice theory.[24] And that in turn has

---

[21] R. Hayes (1991). *Retail Security and Loss Prevention*. Stomham: Butterworth-Heinemann.

[22] For a fuller discussion see, M. Gill and A. Spriggs (2005). *Assessing the Impact of CCTV*, Home Office Research Study 292. London: Home Office. **www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf**.

[23] *The Handbook of Security* (op cite) containing 27 chapters written by experts is a start.

[24] See, Gill, Shoplifters on Shop theft: lessons for retailers. Leicester: Perpetuity Research and Consultancy International. www.perptuitygroup.com/publciations.

led to a set of techniques to reduce opportunities for offenders, known as situational crime prevention.[25] This entails changing the situation or location of a shop, office, workshop, home, to make the crime less likely. The research that exists has formed a foundation on which to build, but there is a lot more to be done to develop the discipline of security properly.

PUBLICATIONS	COURSES
Perpetuity Press PO Box 376 Leicester LE2 3ZZ United Kingdom tel 44(0) 116 270 4186 fax 44 (0) 116 270 7742 email: info@perpetuitypress.co.uk email: dlsc@le.ac.uk	Scarman Centre The Friars 154 Upper New Walk Leicester LE1 7QQ United Kingdom tel: 44 (0) 116 252 3946 fax: 44 (0) 116 252 5766

The Evolving Discipline of Security

Quiz

1. Businesses/retailers are four times more likely to be burglarized then households. ☐ T ☐ F
2. The 1988 British Crime survey found that individuals in certain types of jobs are more likely to become victims of crime. ☐ T ☐ F
3. Crime at the workplace has a direct impact on:
   a) People
   b) Increased costs to consumers
   c) Insurance costs
   d) Health and safety legislation
   e) All of the above
4. _____ is referred to as Security Management.
   a) Crime control
   b) Community safety
   c) Interpersonal violence
   d) Policing
5. One study found that both the public and management hold very favorable views on security in shopping centers. ☐ T ☐ F
6. Evaluations of response to crime whether within an organization or in a community setting need to take into account:
   a) Technology factors
   b) Community standards
   c) Management factors
   d) Policing strategies
   e) A and C
   f) A and B

[25] The whole situational crime prevention approach has been developed by Ron Clarke, for a good discussion of his own defense of criticisms of the topic see, R. V. G. Clarke (2005). Seven misconceptions of situational crime prevention. *In* "Handbook of Crime Prevention" (N. Tilley, Ed.). Collumpton: Devon.

7. Installation of a closed circuit television system can solve all your security problems. ☐ T ☐ F

8. Rational choice perspective refers to:
   a) Organizational studies
   b) How offenders make decisions at the scene
   c) Disaster management
   d) Policy choices

9. The main stages one goes through when planning to tackle crime and other security problems are called the:
   a) Assessment planning techniques
   b) Specific strategy plan
   c) Crime risk management process
   d) Crime issues response

10. Assessment, decision, foci, actions, evaluations are part of the:
    a) Learning process
    b) Security organizational chart
    c) Crime risk management chart
    d) Risk minimization strategy

This page intentionally left blank

2 The Future of Security

David L. Ray and Christopher A. Hertig

Security Industry Trends

"Private security" is now the primary protective resource for citizens in North America. It has been generally held that there are three persons privately employed in the security industry for everyone employed by public law enforcement. This ratio, however, appears to be increasing, but there is a lack of reliable, easily obtainable statistics. As relatively few states license all security personnel, getting an accurate count of them is difficult. In the United States, 85% of the infrastructure is privately owned and controlled. It is protected by "private security" personnel be they proprietary or contract service officers.

It should be noted that the term "private security" is rather vague. While a contract security firm protecting a corporation is clearly "private," the difficulty of applying this label to the same contract firm protecting a military base or stadium is more challenging. While we use the term "private security," we are witnessing a mixture of public and private resources utilized in the protection of our citizenry. This has been the case historically and the individual protection "recipes" will continue to change. What is important to remember is that there will be more privately led, owned, and operated initiatives than in the past. Over the past two decades, the security industry has grown steadily and substantially. It has also diversified and become rather sophisticated in many respects.

The reasons for the trends in growth are complex and varied, but some of the major causes are as follows.

Policing

During the late 1970s and early 1980s, policing in United States grew at a significant rate to keep up with crime trends and with the public's reduced tolerance for crime, especially crimes of violence. With this growth in policing, there was a stronger burden on the federal, state, and municipal tax base. In the late 1980s and early 1990s with the downturn in the economy, the public was no longer willing to accept the tax burden and all government services, including the police, were forced to cut budgets and consequently services.

This downward trend continued into the present time even as the number of police rose: they did so at a pace less than the population growth. Salaries and attendant roll up costs for police are continually escalating. Each contract negotiation between the police officers' union and the government has added to the compensation package for police officers. In 2007, the mean average police salary for a beginning officer in the United States is approximately $40,000. Officers pay increases very rapidly within the first 5 years of employment and they receive shift differential pay. Add to this rapidly escalating health care costs, longer police academy and annual in-service training periods. The cost of public policing is rising!

Pension funds are another major economic issue in some political jurisdictions. The impact of this is not apparent at present but will become so. Lowered earnings than anticipated in pension funds and in some cases a failure by the government to contribute enough into them will surface as major problems in some areas. Underfunded pensions will cost local and state governments plenty in the years ahead. The current move away from defined benefit pension

plans where retirees receive a portion of their highest salaried years for the remainder of their life may accelerate. These plans, however, have been a traditional retention tool of public employers. It is unlikely that they will ever go away completely.

Continuous overseas military commitments by US forces are a further governmental budgetary concern. This will most likely continue due to energy dependence and worldwide terror threats. Having significant numbers of soldiers overseas has several effects. There will be a continued demand for contracted security services in war zones. There will also be a continued demand for private security service providers to replace military police and other government personnel at military installations both within the United States and abroad. There will be a continued drain on public police resources as reserve military personnel get called to active duty. This causes staffing shortages within police agencies; some of which are quite acute. None of them are easily addressed. The Soldiers and Sailors Act requires that the position of someone on active duty be kept open for them on their return. As the hiring of military veterans and reservists is so pervasive in public policing and corrections, those agencies have been forced to cover staffing gaps with officers being paid overtime.

A potential effect of budgetary shortages will be more contracting out to security service firms for those functions that do not absolutely require a sworn law enforcement officer. Contract security officers can guard crime scenes, await the arrival of tow trucks at accident scenes, etc. Public law enforcement, with its continually escalating labor cost spiral, must examine itself more closely. The days of preventative patrol are passing by quickly as governments simply can't afford to have police officers not actively involved in some specific, measurable task. There is greater demand today for police productivity. Levying fines on violators is a measurable activity: some political jurisdictions are increasingly dependent on fines for revenue.

During the past three decades, there has also been a significant increase in commercial property, especially retail shopping malls and office towers. This increase in retail and commercial space has resulted in a corresponding increase in crime at these sites and a requirement on the part of the property owner to provide security for the tenants, retailers, and general public using the facilities. In the same time period, there has also been a revolution in the use of computers by business, and today enterprises of every size rely on computers for their everyday activity. With this reliance on computers came an increase in computer crime that resulted in significant losses every year.

While crime is not the sole issue in information protection, it is a major one. The current concern with identity theft is one example. Identity theft, whether true identity theft or the simple stealing of a credit card number, causes extensive loss. It is now a significant personal protection issue, so much so that one of the authors has begun teaching about identity theft in a self-defense class. Threats to individual citizens have grown beyond rape, robbery, assault, and burglary! In a full-fledged identity/credit capture, the victim may spend 600 or 700 man-hours correcting the problem. This impacts them, their employers, and all the entities they do business with such as banks, credit card companies, mortgage holders, etc. Much of the requisite investigative activity is conducted by privately employed staff from these institutions.

Convergence between physical security and IT has been a buzzword for the past several years. As information loss or dissemination can create an enormous threat to an organization, security departments will become more involved. They will also merge with the trend established after 9/11 for having greater access to top decision makers. Chief security officers are now consulted in more important decisions than ever before; the days of the "company cop" have faded away.

Convergence must occur by necessity as legal issues are involved. Colleges provide one example. College students sending out harassing e-mails to other students may be committing a criminal act. So too would those involved in online scams, gambling, or sex offenses. We have seen many news stories of online sexual predators. While a college campus, for example, may utilize the services of an IT department to address these issues, they are, after all, criminal and the province of the campus police. The campus protection organization must get involved in computer crime prevention, mitigation, and investigation.

Computer crimes also have a cross-jurisdictional aspect to them. Their handling requires the cooperation of various organizations, both public and private, across state, provincial, and national borders.

Information protection will become more complicated. Protection from crime or the malevolent acts of humans only addresses the "C" and "UP" under the WAECUP Model. Waste, Accident, and Error ("W," "A," and "E") are also concerns. As we develop more data bases and become an increasingly information-based economy, our vulnerability expands. There are more information assets to protect, those assets are exposed to more threats and organizations are more dependent on those assets.

The end result is that public law enforcement cannot protect against computer crimes, employee theft or fraud, or drug trafficking in the workplace. They cannot patrol private facilities such as shopping centers, gated communities, manufacturing plants, distribution centers, office buildings, and computer centers. Private citizens and enterprise look to private security services to fill the gap left by the police.

The significant tax burden of policing has caused some small municipalities to contract police services from neighboring jurisdictions. In some cases, regional police associations have been formed for this purpose. These regional departments consist of a regional entity that provides police service (patrol and response) to each of the participating communities on an hourly fee basis. This is contract security except that a government organization is the service provider and policing is the service offered. It is a different means of funding an essential function. Such varied funding mechanisms have been implemented in the past and new ones will undoubtedly develop.

The Justice System and the Courts

The court system has also contributed to the rise in the use of "private" security. There has been a general reduction in the perception of efficiency in the justice system as a result of lengthy delays in cases going to trial, a view that the courts favor the accused person rather than the victim and the prohibitive cost of criminal litigation. This lack of public confidence causes a greater need on the part of the public and private enterprises to ensure that systems are in place to deter crime before it happens rather than force the business to become involved in protracted criminal or civil proceedings. One noteworthy development has been the widespread use of civil recovery, particularly by merchants in the United States.

Civil recovery or civil demand varies by state and is generally limited to thefts of merchandise from retail establishments. It may well be that civil recovery will be made available as an option for various types of crimes that are economic and difficult for the criminal justice system to deal with. Commercial counterfeiting, embezzlement, and fraud may be written into statutes that allow the victims to seek financial recovery through a civil demand process. This will bear close watching in the next decade.

"Street Crime"

Another reason for the rise in demand for private security is the general perception of crime trends. Violent "street crime" is at the forefront of that perception. While crime rates may have leveled off, the perception of crime has increased. Whatever the true rate of crime, the public believes that it is getting worse. As a result, they are more apt to purchase security services.

Business also suffers where a third party is victimized on company property. The marketing activity of getting more shoppers, more tenants, and more visitors has another side to it: responsibility for their safety. Security- and crime-related lawsuits have become commonplace. As a result, businesses are protecting themselves against legal actions by providing stronger deterrent measures against crime on their premises. Protective measures that were once not seriously considered are now being budgeted for.

Cultural Changes

Demographics and culture are playing a major role in Asset Protection. Increasing immigration in many areas creates a host of challenges. Dealing with different cultures and languages forces security personnel to learn about the different cultures, maintain surveillance of them without being

prejudiced against them, etc. Discriminatory treatment of differing ethnic groups, particularly but by no means exclusively, Muslims, is not acceptable. The use of more sophisticated behavioral profiling may be part of the answer; one we may borrow from our Israeli colleagues.

We are witnessing a massive increase in the number of elderly persons. Long-term care facilities are expanding in size and number. Retirement communities are in many instances small cities; isolated, contained, and complex having shopping, entertainment, and health care all within their confines. Emergency planning, internal theft, fraud, and abuse of residents are all concerns. Security of long-term care facilities will become a greater issue and more people will be employed within that sector.

Workplace values and expectations are different. Tulgan and RainmakerThinking (2003) studied the generational shift in the workplace from 1993 to 2003. They found that work has changed as have the perceptions of newer employees. Findings directly relevant to security include the following:

1. Work has become more demanding on employees, many of whom feel "burnt out."
2. Employees are more focused on short-term rewards than "paying their dues"; they feel as though their employment may be temporary rather than permanent.
3. Supervision of employees is more challenging, time consuming, and important. Part of the reason is a more diverse workforce. Another is that employees feel that they need more coaching from supervisors.

Some workplace problems are security problems. Others evolve into becoming security problems. The changing nature of the workplace will be a constant challenge to protect professionals at all levels.

Economic Crime and Terrorism

Economic crime, most of it involving the workplace, will continue to evolve. It is profitable and can take a myriad of forms. The passing of bogus checks, shoplifting, embezzlement, and phishing are all economic crimes. So too are workman's compensation fraud, commercial counterfeiting, and refund fraud. Some crimes are simple, others are sophisticated. As the economy transforms, so too does the type of victimization.

A focus on terrorism by some governmental investigative agencies may make for less hardening of economic targets. Large-scale fraud may become a greater threat, at least from an economic perspective, than acts of terror. Additionally, focusing on organized terror groups does little to prevent actions by kooks and "lone wolves." Kooks are mentally deranged persons, devoid of any discernable political or social agenda. They create terror through acts of violence but are not terrorists according to most common definitions. They are quite numerous, at least in the United States. The "workplace avenger" who returns to his or her place of employment and shoots his or her supervisor being but one variety.

"Lone wolves" have a political or social agenda but operate on their own. They may have belonged to a group at one point in time but are no longer members. They are, like kooks, difficult to track through routine intelligence activity. Like kooks, they are numerous.

One bright spot may be that the development of task forces for dealing with terrorism, Organized Retail Crime, and other issues will create new investigative and response mechanisms. These may be of use in identifying, monitoring, and intercepting all manner of malevolent persons, be they members of organized criminal groups or individuals acting alone. Interagency task forces will probably be more common than at present. We will certainly see a greater emphasis on analytical software. Quantitative analysis applications for both proactive and reactive intelligence will be used more. This trend will segue in with the expectations of corporate upper management for metrics on all manner of activities: "intel" meets business!

The events of 9/11 and the US invasion of Afghanistan marked the beginning of a new era regarding Islamic fundamentalism. Civilized nations in general and Western democracies in particular will be waging a multifaceted campaign against radical Islamic fanatics for decades to come. Whether one refers to this as "The War on Terror," "The Long War," or "The Era of Asymmetrical Warfare" is a point of academic discussion; the struggle will continue.

Cyber terrorism will evolve. The popular view may be that cyber terror is not a pressing problem; that it is not in Al-Qaeda's style to conduct such operations. Unfortunately, there

have been indicators of interest in cyber terror by Al-Qaeda. There have also been numerous instances of cyber crime such as denial of service attacks, viruses, etc. These have been perpetrated against individual organizations and have not gotten into or remained in the media spotlight for very long. The "smoke" is there, if not the "fire." It is only reasonable to conclude that cyber attacks will escalate in severity at some future point. While not as spectacular as suicide bombings, they can have enormous economic impact on an individual organization. The stakeholders of the organization be they customers, clients, employees, or patients are also affected. Cyber attacks can damage physical infrastructure and are part of the military options of nations. A 9/11-style attack perpetrated through cyberspace would have grave consequences.

Ecoterror will continue to increase. These groups have demonstrated an increasing degree of violence and sophistication over the past several decades. Historically, much of the activities of these groups has been "under the radar." They do not get mainstream media attention as suicide bombing has not been in their modus operandi. Ecoterrorists have become a sophisticated left-wing phenomenon harassing corporations, their officers, employees, customers, and suppliers. They have international connections and a substantial degree of popular support. Their actions are not spectacular, but costly from an economic perspective. Intimidation is another cost entirely.

Trends in Business

The last reason for the upswing in the use of private security is the general economic conditions over recent years and trends in business. Businesses are seeing reduced profit margins and possibility of financial failure (e.g., a conservative estimate is that one out of three small businesses fail because of employee theft). As a result, there is a stronger recognition of the need to protect assets.

> *The first duty of business is to survive and the guiding principle of business and economics is not the maximization of profit it is the avoidance of loss.*
> —Peter Drucker

Another growing phenomenon is the trend to outsource the noncore area of an enterprise. If a need is established for more security within an organization, there is now a greater likelihood that the organization will approach a security service to provide it rather than hiring internal staff to provide the service. Commensurate with this customer demand has been a growth in sophistication on the part of security service providers. These firms are showing increasing managerial acuity in terms of cost containment, marketing, employee recruitment, training, etc. The contract services sector is clearly maturing.

Economic Conditions

Security Management provides some challenges under poor economic conditions. Economic crimes tend to increase because people are strapped for money. Corporations suffer from reduced morale, and those intent on theft or fraud find it easier to justify their actions. Insurance costs increase and often companies are forced to take on larger deductibles. Insurers are also not as quick to settle claims and may dispute them.

Litigation increases because companies are seen to have deep pockets and because legal firms are more willing to take clients under a contingency fee arrangement. Environmental legislation also places a strain on budgets. Security departments are generally asked to do more with less and shed all but nonessential services. The need to partner with different departments as well as the necessity of defining operational parameters is increasing.

The strain on corporate budgets, the changing nature of crime in the workplace, and the increased cost of litigation have created a greater necessity for security departments to become involved in the following:

- Background checks on new or potential employees are becoming much more prevalent
- Training of both security and nonsecurity employees to avoid false arrest, malicious prosecution claims, and claims of failure to provide adequate security
- Programs to protect employees against workplace violence

- Investigations into compliance with environmental legislation
- Investigations into workplace infractions
- Follow up investigations from whistle blowing
- Drug testing
- Contingency planning as emergencies and disasters are growing concerns of both private and public organizations

Nature of the Security Industry: The Future

What is the future of security services? Predicting the future is never an exact undertaking, but a review of historical and current trends provides some insight. A few developments are outlined below.

1. Outsourcing will continue as a significant initiative.
   Corporations will continue to work hard at reducing overhead and operating costs by hiring contracted services. The Hallcrest study found that between 1990 and 1993 there were 800 fewer in-house security departments in operation in United States, and there were layoffs of ~22,000 proprietary security personnel. From the late 1990s onward, the trend appears to be an emphasis on quality rather than price. Clients seem more willing to pay premium fees for premium services.
2. Private security will continue to provide cost-effective protection measures.
   Availability will be high and competition among security suppliers will continue to provide value. Technology will continue to play an increasing role and technology costs will continue to drop. There will be increased supply of security services to fill an increasing demand. This demand will be from both private and public organizations; the use of CCTV by communities in the United Kingdom as well as in United States is but one example.
3. Security will continue to erode the role of law enforcement.
   Over time, law enforcement will continue to be under pressure to keep budgets in control. This will cause them to focus on those activities that most require their services and those where there is a high public expectation of response. These will especially include investigations into robberies, sex offences, weapons-related offences, and other crimes of violence. They will not have the resources to continue with extensive patrols, especially of private property, and they will place a greater expectation on businesses to provide internal investigation of white-collar crime.
4. There will be continued demand placed on in-house security directors.
   - A stronger expectation to justify expenditures
   - More educated
   - Broader range of management skills for both proprietary and contract managers
   - Integration with other departments such as facilities, HR, risk management, or audit departments
   - Expectation to do more with less
   - Better communicators
   - Stronger computer skills
   - Flexibility and adaptability
5. Equipment sales and revenues will continue to be strong.
   Surveillance and access control systems have seen robust growth in the past decade or so and this trend will continue. New technology for signal transmission will have an impact. A serious consideration is public expectation: organizations will be expected to have security equipment as it will become more commonplace.
6. Power outages in the United States will become more common.
   A greater demand for power, degradation of the power grid, and a lack of power generation facilities are major drivers for this. Both natural disasters and human error can trigger outages. There are initiatives underway for greater power generation from coal and other sources. While not nuclear, these power plants will still need the

services of those involved in protection. Planning, protecting, and complying with regulations are all part of the package.

7. Natural disasters are gaining extensive coverage in the news media. Traditionally, crime has got public attention through both the news and entertainment media. Fear of natural disasters will, to some degree, replace fear of crime as a driver for the purchase of security products and services. Human-caused catastrophes will be part of the mix. Historically, they have not had the widespread impact of natural disasters but this may change. Proprietary security departments will have more demands placed on them to be involved in emergency planning, response, and recovery. Contract service firms will have more opportunities to provide unique, specialized services of a critical nature.

Legal Concerns

Increased legal requirements are evident. More licensing and training standards for contract security personnel will evolve over time. Generally, this has been at the state or provincial level and the passage of such legislation takes several years. Also the training requirements are minimal and the laws only cover contract personnel, not in-house. Of note is the fact that both California and Ontario regulate proprietary security personnel as well as contract. This is certainly needed but rarely undertaken by state or provincial governments. The developments in Ontario and California may begin a trend. Such legislation can have a profound impact on the security industry: no longer will just anyone be able to work in it. Everyone will have to have some type of training and licensing in order to be employed.

Increased legal standards in terms of requirements by governments as well as non-profit professional groups. Standards and guidelines are being developed by local, state, and national governments regarding the protection of assets. Laws requiring organizations to protect customer data are one example. Organizations such as ASIS International and the National Fire Protection Association are coming out with guidelines and standards at a rapid pace. This will have a major impact on the business of protection. Organizations will require a "Security Manager" or a "Compliance Manager" within a few years. Employers that don't currently have these positions will need to adapt. Those that have the appropriate staffing will be tasked to do more. Outsourcing of compliance functions via subscription services, audits, etc. is a distinct possibility and service firms have moved into that market. Currently, there are publications being produced to address this issue.

Education

Education is a necessity for the development of any profession. Security cannot afford to become the exception. Fortunately, there are a variety of educational developments at the professional, secondary, undergraduate, and graduate levels. Professional organizations such as the International Foundation for Cultural Property Protection, ASIS International, the International Association of Health care Security and Safety, the International Association of Law Enforcement Administrators, and many others have developed ongoing professional educational processes for their members. These programs include seminars, publications, online courses, and professional certification processes.

Protective Services programs at the secondary school level have taken hold in the United States. The National Partnership for Careers in Law, Public Safety, Corrections, and Security has served as a clearinghouse for these programs. Protective Services curricula prepare students to go to college, the military, or begin careers in policing, security, fire protection, or emergency medicine. It would appear that the earlier emphasis on policing has given way to a more well-rounded security/emergency management approach. A growing number of these schools are using the Certified Protection Officer (CPO) program as a means of outcome assessment for their graduates.

Undergraduate degree programs in security have not shown dramatic growth within the United States. Teenagers and young adults simply don't see the "Invisible Empire" of private

security, at least not until they begin the job search. There probably needs to be a closer relationship with Criminal Justice programs, an integration of courses so that students see what the security industry has to offer. There has, however, been growing interest in Security degree programs due to the events of 9/11. Current initiatives by the ASIS International Council on Academic Programs will aid in developing this interest.

In Europe, there has been growth in undergraduate Security programs. There are both degree and nondegree courses offered for security practitioners. European universities have also partnered with security professionals and organizations to merge academia with professional certification. Jack Valk and others have taken a leading role in this effort.

There are also a number of online degree options occurring. These online programs have generally been oriented to the needs of working professionals rather than traditional college age students. They may, however, become part of "the Big Picture" of academia. They have the potential to play a leading role within it.

An education evolution is inevitable with private online colleges. A current trend in the United States is for students to take their first 2 years of study at a community college where the tuition is much lower. In some cases, the community colleges are growing into 4-year programs, thereby taking a substantial portion of the student market away from established 4-year institutions. Online programs will evolve that are attractive and user-friendly to traditional college age students as well as the faculty that must teach them. These programs will have widespread market acceptance.

The net result is that there will be winners and losers among institutions of higher education. Transfer of courses will be an even greater issue than it is at present.

Homeland Security programs at colleges in the United States have grown to number of ~300. Much of the impetus behind their implementation has been the receipt of federal monies. The other driver is the popularity of "Homeland Security," however that term is defined. There is some concern about whether this is a valid area for academic study. Another concern is whether there are jobs waiting for graduates. Fortunately, much of the curriculum in Homeland Security is within Emergency Management. Some of it is within security management. Both of these are valid fields with numerous employment options for graduates. Both emergency management and security management are part of the core competencies for emergency managers, security managers, police chiefs, fire chiefs, etc. One may not have "Homeland Security" or "Emergency Management" in their job title; but they will have it within their job description. Add to this, courses in terrorism and counterterrorism and it can be argued that a Homeland Security degree recipient is fairly well versed to move into management jobs with both public and private organizations. The career competencies are present; the career path is less visible.

The prevalence of security management coursework within Homeland Security programs remains to be seen. It is perhaps too early to easily discern what direction these programs will take. Some may evolve into security management or emergency management curricula. Whatever occurs, Homeland Security courses will drive research efforts. Methodology for assessing and managing risks is being developed and studied.

At the graduate level, security management has fared well. The more mature student sees a viable career ladder and is more focused on learning. Curriculums are easily designed as graduate education generally has management components within it. Taking those existing courses and adding a few Security courses is simple from a program development standpoint. Additionally, an interdisciplinary perspective is easily achieved at the graduate level. A program on Retail Loss Prevention, Homeland Security, Risk Management, or IT Security can be rolled out fairly easily in many cases. Certificate rather than degree programs may be particularly appropriate. There are many well-known institutions of higher education offering graduate degrees and certificates in some facet of security management. In the future, these programs will be increasingly common. They will be increasingly online in delivery and international in content.

Research

The security industry has traditionally not been heavily tied to research, particularly in the United States. Our European and Canadian colleagues have certainly led in the research

realm with quality work being done by major universities, the Perpetuity Group, and other organizations. This research must be shared and embraced. The criticality of security-related threats requires scientific study from a multidisciplinary perspective.

Theoretically, Homeland Security deals with the domestic efforts to defend United States from terrorist attack. In the practical sphere, these efforts also encompass general preparedness for terrorism, natural disasters, hazmat incidents, and pandemics. It is an "all hazards doctrine." And it will require input from governmental entities, insurance carriers, IT researchers, and public health professionals, among others. There will, of necessity, be more research on dealing with substantial man-made and naturally occurring problems. The research will be interdisciplinary; no longer will the security industry be married solely to policing and the military. There will be other partners. The chapter on Accident Causation Theory is an example of how security can utilize methodologies from related disciplines.

Currently, there are a variety of research efforts underway including the following:

- The ASIS Foundation is sponsoring a variety of research projects as well as the Academic-Practitioner Symposium; an annual meeting of leading researchers, academics, authors, and security practitioners.
- The peer-reviewed *Security Journal* is published by Palgrave MacMillan and affiliated with ASIS International. It contains scholarly papers authored by leading researchers from around the world.
- The *Journal of Physical Security* is an online peer-reviewed scholarly journal focusing on the technical or social science components of physical security.
- *Retail Crime, Security & Loss Prevention: An Encyclopedic Reference* by Sennewald and Christman and published by Butterworth-Heinemann. The book has contributions from 63 different authors, offering a myriad of perspectives on retail loss issues.
- The *Encyclopedia on International Security Studies* by Congressional Quarterly Press. This book consists of ~800 entries. It is a merging of public and international security concerns such as national security and military issues with "private security" topics.
- The Perpetuity Group, which offers training and consulting in the areas of crime risk management, also publishes research-oriented books and journals.
- The International Foundation for Protection Officers offers the Article Archives, an online repository for research papers. The archives' materials support and expand on printed Foundation programs.

Conclusion

Overall there will be continued demand for security measures in the foreseeable future. The impetus for this will be from the risks associated with terrorism, organized criminal activity, natural disasters, and man-made catastrophic events.

Population density and the economic interconnectedness of our society make us vulnerable to problems extending over a large geographic area or that enters our communications networks.

The expectations and demands of the public we serve as well as governmental and nonprofit organizations will drive the industry. General managers and security managers will be asked why their organizations don't employ the same measures as similar entities do. Stakeholders will question the security measures taken to a larger degree. Statutes and standards will also impact on security management in a major way.

Information protection will continue to be a major concern. Those security departments that can embrace it will thrive, those that don't will be marginalized within the parent or client organization.

Greater and more diverse responsibilities will be given to security professionals, especially those at the supervisory and managerial levels. Those professionals must be committed to their profession and adaptable to change. They must welcome "having more put on their plates."

Security management and asset protection will develop into more mature professional disciplines allied with other fields of study and based on research efforts. Substantial decisions having major organizational impact cannot be based on guesswork.

Continuing professional development will be the norm. Practitioners will be more likely to need preservice training due to government or employer-initiated requirements. Once employed, annual in-service training will be required more so than in the past. Professional certification processes will be completed by an increasing number of personnel; these processes require periodic recertification. Management level personnel will need to hold academic degrees; graduate degrees will be more in demand for those ascending the "corporate ladder."

References

W. Cunningham and T. Taylor (1985). *Private Security and Police in America: The Hallcrest Report I*. Portland, Or: Chancellor Press.

W. Cunningham, J. Strauchs, and C. Van Meter (1990). *Private Security Trends 1970–2000: The Hallcrest Report II*. Boston, MA: Butterworth-Heinemann.

M. A. Sauter and J. J. Carafino (2005). *Homeland Security: A Complete Guide to Understanding, Preventing, and Surviving Terrorism*. New York, NY: McGraw-Hill.

B. Tulgan and RainmakerThinking, Inc. (2003). *Generational Shift: What We Saw at the Workplace Revolution*. RainmakerThinking, Inc.

J. Rogin (2007). Attack by Korean Hacker Prompts Defense Department Cyber Debate. FCW.com News. http://www.fcw.com/article97645-02-09-07-Web accessed on February 14, 2007.

The Future of Security Quiz

1. Merchants in the United States use _____ to recover money from shoplifters. This may spread to other types of economic crime.
2. Security will continue to erode the role of _____.
3. Natural disasters may become major drivers for the purchase of security products and services. They may replace _____ to some degree in the news media.
4. Homeland Security has theoretically focused on prevention and response to _____. In practice it has expanded to encompass dealing with natural and man-made disasters.
5. _____ terrorists have international connections, have not engaged in spectacular attacks, and are very sophisticated.
   a. Islamic fundamentalists
   b. Ecoterror groups
   c. Kooks
   d. "Lone Wolves"
6. There are two times as many security personnel as police personnel. This ratio is staying the same. ☐ T ☐ F
7. Organizations will need to hire either security managers or compliance managers in order to keep abreast of increasing governmental and private regulatory efforts. ☐ T ☐ F
8. Organized Retail Crime is an interjurisdictional problem requiring the use of public-private task forces. ☐ T ☐ F
9. There are 300 colleges in the United States offering Homeland Security courses or degree programs. ☐ T ☐ F
10. Security managers will most likely avoid combining security programs with other departments within an organization. ☐ T ☐ F

APPENDIX: The Future of Security Training

Jeffrey A. Slotnick

Concepts

Our world is continually changing. This has resulted in a period of dynamic change within the security industry. Just turn on the news this morning and you will find several world events with significant impact are occurring.

There is a war going on, violence in the workplace, and hate-related crimes are rampant. Bomb threats and threats of terrorist activity are a daily occurrence.

This does not consider such minor day-to-day issues as gang wars at our malls, entrepreneurial criminals working in groups to target industries, several bank robberies, and situations involving workplace violence.

The common thread in each one of these events is the presence of a Security Officer nearby or on scene. But you have to ask yourself were these guards trained properly, are they properly supervised, and given all the tools they require for professionally responding, helping others, and surviving.

The 106th Congress of the United States published the following in their *Security Officer Quality Assurance Report:*

> *Private security officers are much more prominent in society today than years ago. Members of the public are increasingly likely to have contact with these individuals and often mistake them for law enforcement officers. It is important that private security officers are qualified, well-trained individuals to supplement the work of sworn law enforcement officers, further the American public demands the employment of qualified, well-trained private security personnel as an adjunct, but not a replacement for sworn law enforcement officers.*

Minimum Standards

There are 21 states that require prelicensing training, but only 8 that require postlicensing training.

Because of the varying duties within the industry, many train to a one-size-fits-all standard that is based on minimum qualifications. The highest standard in the United States requires only 40 hours of preassignment training.

The problem with this type of training is very simple: you get what you pay for. Minimum standards lead to minimum performance, this in kown as Lowest Common Denominator Training.[1]

> *You won't rise to the occasion—you'll default to your level of training.*
> —Barrett Tillman, *The Sixth Battle*

Anyone in the training industry will agree, when you get into a stress or critical response situation you will resort to the training you have received. This is a subconscious process over which we have no control, it is acting by instinct. With this in mind, training has to focus on the expected response.

Ken Good of Strategos International[1] states:

> *Intuitive responses are something you default to quickly without sequential/conscious thinking, as a result of experience. Intuition based on experience is generally very reliable and in fact a necessity in critical, high-stress situations.*

---

[1] (C) J. Ken (2006). Good, Strategos International LLC. Reprinted with permission. Please visit www.strategosintl.com.

So what is the response? The days of the .38 Special carrying bank guard are long gone. In today's industry, security officer's duties and responsibilities change with each post. Additionally, higher threat levels for varying positions and locations may dictate higher levels of competence.

Here are some examples of varying positions:

Bank Robbery Suppression	Facility Concierge
Retail Loss Pr ntion	Downtown Bicycle Patrol
Alarm Response Patrol	Shopping Mall Security
Military Installation Portal Security	Hotel Security
Federal Building Security	Casino Security
High Rise Security	Nuclear Site Security
Port Security	Transportation Security

So how do we as an industry determine the training standards for all these varied assignments? There are two methods: Job Task Analysis and the Mission Essential Task Lists (METL, pronounced metal) Approach.

Job Task Analysis

Job task analysis is the process of identifying and determining in detail the particular job duties and requirements and the relative importance of these duties for a given job. The purpose of a job analysis is to establish and document employment procedures such as training and selection.

This usually will guide you toward developing your training program and allows you to consider the content of your training.

Determining Training Needs

Job Analysis can be used in training/"needs assessment" to identify or develop:

- Training content
- Specific curriculums
- Assessment tests to measure effectiveness of training
- Equipment to be used in delivering the training
- Methods of training (i.e., small group, computer-based, video, classroom …)

METL Approach

The US military provides an excellent model for this method. The METL approach is a tool used by war fighters to link training to mission. What is METL? Army Field Manuals FM 25–100, Training the Force, and FM 25–101, Battle Focused Training are Army's doctrinal sources for METL. The METL "tool" enables the war-fighting commander to focus training on tasks essential to accomplishing the organization's wartime mission. Specifically, the extended METL process enables commanders to identify those tasks most critical to wartime mission accomplishment, to assess the training level of soldiers against those tasks, and then to develop a training plan that focuses limited resources (time, people, and money) against those tasks.

This same capability applied to the security industry will prove invaluable during this time of dynamic change.

Due Diligence

Another aspect to consider is the legal and insurance implications in this process. In our industry, we know these as due diligence and maintenance of effort.

The Webster's Dictionary defines "due diligence" as "the care that a reasonable person exercises under the circumstances to avoid harm to other persons or their property."

Maintenance of Effort defined, generally, the term "maintenance of effort" implies spending the same or a greater amount of effort and funds to maintain programs and services from one fiscal year to the next.

In the past 4 years, we have served as an expert witness in numerous lawsuits where security officers failed to act or acted improperly. In many of these cases, management either did not perform a proper background check of the employee or failed to provide adequate training for the duties and responsibilities of the position. All the cases settled for between $300 and $500,000 and involved personal injury.

Failing to prepare is preparing for failure.
—John Wooden

So Where do We Go from Here?

In the past several years, the federal government has produced several documents that are integral to our industry and provide a template for action. These documents are the National Infrastructure Protection Plan (NIPP) and the National Response Plan (NRP).

The NIPP http://www.dhs.gov/interweb/assetlibrary/NIPP_Plan.pdf provides a coordinated approach to critical infrastructure and key resource protection roles and responsibilities for federal, state, local, tribal, and private sector security partners. The NIPP sets national priorities, goals, and requirements for effective distribution of funding and resources which will help ensure that our government, economy, and public services continue in the event of a terrorist attack or other disaster.

The plan is based on the following:

- Strong public–private partnerships, which will foster relationships and facilitate coordination within and across critical infrastructure and key resource sectors
- Robust multidirectional information sharing, which will enhance the ability to assess risks, make prudent security investments, and take protective action
- Risk managemnt framework establishing processes for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector risk

Some of the principle imperatives of the plan include the following:

- Implement measures to reduce risk and mitigate deficiencies and vulnerabilities corresponding to the physical, cyber, and human security elements of CI/KR protection
- Maintain the tools, capabilities, and protocols necessary to provide an appropriate level of monitoring of networks, systems, or a facility and its immediate surroundings to detect possible insider and external threats
- Develop and implement personnel screening programs to the extent feasible for personnel working in sensitive positions

Additionally, the NIPP does not solely consider terrorist activities but includes an "all hazards approach" to resiliency. All hazards mean that the federal government weights a response to a natural or man-made disaster equally to a terrorist or criminal event.

National Response Plan

The NRP, http://www.dhs.gov/interweb/assetlibrary/NRP_FullText.pdf last updated May 25, 2006, establishes a comprehensive all-hazards approach to enhance the ability of the United States to manage domestic incidents. The plan incorporates best practices and procedures from incident management disciplines—homeland security, emergency management, law enforcement, firefighting, public works, public health, responder, and recovery worker health and safety, emergency medical services, and the private sector—and integrates them into a

unified structure. It forms the basis of how the federal government coordinates with state, local, and tribal governments and the private sector during incidents. It establishes protocols to help:

- Save lives and protect the health and safety of the public, responders, and recovery workers
- Ensure security of the homeland
- Prevent an imminent incident, including acts of terrorism, from occurring
- Protect and restore critical infrastructure and key resources
- Conduct law enforcement investigations to resolve the incident, apprehend the perpetrators, and collect and preserve evidence for prosecution and/or attribution
- Protect property and mitigate damages and impacts to individuals, communities, and the environment
- Facilitate recovery of individuals, families, businesses, governments, and the environment

Private sector as a response resource extracted from the NRP; private sector organizations are encouraged to develop and maintain capabilities to respond to and manage a complete spectrum of incidents and emergencies. The federal government maintains ongoing interaction with the critical infrastructure and key resources industries to provide coordination for prevention, preparedness, response, and recovery activities.

Based on the above, there are several areas of concentration which should be considered for future training of all Security Officers:

- Detecting criminal and terrorist activity through surveillance
- Technology and Smart Systems
- Training in the National Incident Management System (NIMS) and the Incident Command System (ICS); both of these courses are available online and free of charge at http://www.training.fema.gov/EMIWeb/IS/crslist.asp. As a minimum, Security Officers should consider taking IS100 and IS700. Additionally, there are a number of infrastructure-specific courses free of charge at this same Web site.

DHS Course, UNLV Frontline Responder Training Course Terrorism Awareness: Protecting Soft Targets

This course is available online at http://education.unlv.edu/Educational_Leadership/Ed_Leadership_web/cwd/frontline/course_info.html. In this course, you can gain knowledge in eight separate modules that can be delivered separately or as a package over 2 days. The course is realistic, written by subject matter experts in your industries. This course uses a blended learning methodology, combining instructor-led training, role-playing, scenario enactments, group discussions, and demonstrations.

The modules include:

- Terrorism awareness: the definition of terrorism, categories and types of terrorism, targets, types of threats, and the DHS threat advisory system
- Homeland Security role: The DHS mission statement and strategies developed for domestic and national preparedness
- Weapons of mass destruction: The properties, effects, and methods for delivery/dispersal of potential CBRNE agents. Personal protection principles for radiological and explosive incidents
- Improvised explosive devices (IEDs): The basic design of IEDs including vehicle-borne IEDs and suicide bombers
    - Terrorist planning cycle and suspicious person indicators: The terrorist operational planning cycle and suspicious person indicators

- Suspicious items indicators and types of threats: Common types of threats (bomb threat, found package, etc.) and practical ways to handle these threats
- Incident scene management: The strategic goals of incident management, as well as an overview of the unified ICS
- Soft target assets and vulnerabilities: An awareness of the physical structure, building grounds, occupant routines, and physical security systems in soft target properties

This particular course is invaluable to those who are charged with the protection of soft targets and critical infrastructure.

Public–Private Partnerships

Both the NIPP and NRP call for involvement of the private sector. Security Officers, Security Supervisors, and owners of Security Companies certainly come under the heading of private sector.

Get involved in local forums that discuss area concerns and warnings. On a national level, there is the United States Public Private Partnerships (USP3) Program hosted by the FBI with local governance. There are a number of regional groups where you can be involved. Learn more about this program at http://www.usp3.org/.

Additionally, in local areas there are Public/Private Threat Early Warning groups that exchange important information on area threats and concerns. Included in these partnerships are many Information Sharing and Analysis Centers (ISACS); these organizations are generally specific to sectors of infrastructure.

Finally, as another resource many states have Emergency Management Agencies and Colleges that sponsor Homeland Security Centers of Excellence. These organizations generally host a number of DHS-funded training course that are specific for our industry. The only expense is the time to get trained.

In closing, the status quo is no longer acceptable; we never know when a disaster either man-made or natural will occur. Should one of these events happen, can you honestly say that you have done everything within your financial ability and time constraints to provide your personnel what they need to respond with confidence and competence. It is no longer about the Least Common Denominator; it is about being representatives for excellence in our industry and facilitators of change.

Quiz

1. Private Security will continue to provide _____ _____ protective measures.
2. Security will continue to erode the role of _____ _____.
3. By the year 2000, it is predicted that the national budget for law enforcement will be _____ _____.
4. By the year 2000, it is predicted that the national budget for private security will be _____ _____.
5. In the U.S., it is estimated that business is losing _____ annually as a result of crime.
6. There are two and one half times as many security personnel as police personnel. ☐ T ☐ F
7. The University of Minnesota study on theft by employees in work organizations established that theft will take place just as often even if there is a prosecution policy. ☐ T ☐ F

8. The average "take" in a computer crime is $500,000. ☐ T ☐ F
9. The Brigham Young study on white collar crime established that while collar criminals were more likely to be women. ☐ T ☐ F
10. There is more likely to be an expectation that security managers will avoid combining security programs with other departments within an organization. ☐ T ☐ F

3 Key Terms and Concepts

Robert Metscher

What better place can there be to begin training as a security supervisor or manager than with words? Words provide the foundation for sharing written and spoken ideas. They are a fundamental building block of learning and communication. So, could there be a better place from which to begin the journey of professional development than to understand the most fundamental unit of that training? Possibly so, however, here it provides a short introduction and context for much that will be learned in a career in security.

Security is a young discipline with its modern roots in the industrial security programs that came about from the Second World War, and this is significant because there are few, if any, true standards. This is certainly no more apparent than in the vernacular of its practitioners. There is occasionally heated discussion over what is the appropriate terminology for different aspects of the profession. With that said, it is as important to understand the terms discussed in this chapter as it is to understand the underlying concepts to prevent any confusion when others use different terms.

Today, the security supervisor or manager is expected to operate and provide leadership within an organization beyond that of just being a more prominent security officer. One should be conversant in business and organizational concepts such as management techniques, risk management, crisis management, human resources (HR) management, legal issues, and public relations just to name a few. And before reaching for this knowledge, it is essential to understand terms associated with the character of successful supervisors and managers found in the Protection Officer Code of Ethics. Terms like integrity, confidentiality, honesty, discipline, and rapport define the conduct of a security professional.

Security supervisors and managers should be well versed in common security-related concepts. Understanding these concepts permits the security professional to function among peers that may use an entirely different set of terms to describe the same ideas. Why does this happen? Simple. Security is an immature discipline with limited formal governance. While organizations like ASIS International (formerly the American Society for Industrial Security) and the International Foundation for Protection Officers strive to create some order in this sea of chaos, they are but two of many organizations, thinkers, and authors that are writing the rules of future security. In addition to knowing basic concepts, the security professional should have an understanding of the security industry as a whole. This includes knowing the segments of our industry knowledge such as physical security, information security, and personnel security to name just few. There are many others that a little research on the web will quickly reveal. Bear in mind that there is overlap in these segments, for instance does the document containing sensitive information fall within a physical security program or the information security program? And the answer often depends on the organization's desires or an arbitrary divide created for a presentation. Additionally, a security profession should be aware and at the very least have some knowledge of the various operational services offered by the industry, including proprietary/contract uniformed services, private investigations, cash-in-transit (armored car), internal investigations, fraud auditing, undercover investigations, emergency response, as well as many more. Even mild involvement in local security industry events will expose an inquisitive individual to much of this information.

As the security professional moves from the role of protection officer to that of a security leader, so too does the nature of the knowledge needed to be effective. Security knowledge now begins to shift to planning, operations management, and organizational advice. To do this well, the security professional must learn about organizations, their functional segments, and how they operate. What does a marketing department do? What exactly is marketing and how is it different from accounting, payroll, HR, or security? Fundamental knowledge of the organization permits the security professional to better mesh with other business professionals and to guide the organization to the most appropriate level of security. A security professional that presents a security plan without an understanding of the budgetary, personnel, or operations impact is unlikely to gain much support from top management.

Commerce, Supply and Demand, and Stakeholders

Business organizations, not-for-profit organizations, and government agencies are fundamentally different in their function and operation. While all of them require money to function, they obtain them in very different ways. Governments obtain funds through the taxation of a population and businesses earn funds through commerce. Commerce is the voluntary exchange of goods and services between parties for mutual gain. It is voluntary and therefore occurs without coercion, or the use or threat of use of force. The common tool of exchange is money. Money represents stored value that may be used in the future. It is typically obtained by providing a good or service. A person works at his job and receives pay for his labor. They in turn spend this money on items, such as food, which they are unable or unwilling to produce themselves. Money then is the stored value of their labor. Organizations operate on a grander scale but the concept remains the same. A good or service is provided in exchange for money. The value of the good or service is decided by the market forces of supply and demand. The basis for this concept of supply and demand assumes that all resources are limited. Too much supply and the price goes down, while too little supply and the price increases. Demand operates inversely with excessive demand driving the price up and reduced demand resulting in lowered prices. Consider trying to sell a car. If there were no other cars available for sale and many people wanted your car, the price would be much higher than if there were many other cars available for sale or very few people were interested in purchasing the car.

Events and decisions within an organization affect individuals and groups. These individuals can be referred to as stakeholders. This sounds similar to shareholders but is much broader. A shareholder is a person, or organization, that owns one or more shares of stock in a business and so is a partial owner of the company. A stakeholder is any person or organization that has a stake in an organization, event, decision, or plan. Stakeholders include suppliers/vendors, customers, owners, managers, employees, and so on. The security professional must be able to identify the various stakeholders in their decisions, actions, plans, and proposals. Requests for funds affect others within the organization that are competing for the same scarce funds. Changing the access procedures for a facility affects all that need access and may affect the timing of production timelines and utility costs. Identifying stakeholders in advance permits the knowledgeable security professional to present value or importance for each perspective.

Management and Management Methodology

One significant group of stakeholders is the managers of an organization. Managers are those that are responsible for the performance of an organization, or the function of management is to maximize the performance of the organization. In businesses, performance should maximize the wealth of the owners. The owners are, of course, the shareholders and wealth is a long-term goal that differs from profits. Profits are the rewards for a specific amount of effort, while wealth encompasses current profits and any future profit. Government and not-for-profit organizations' performance is measured in the quality of the services provided and, as we hear continuous stories of waste, is generally not measured on efficiency.

Management then is responsible for organizational performance but not necessarily for performing the actual tasks that account for that performance. Managing is commonly

thought to include several functions, including planning, organizing, staffing, directing, and controlling activities. Security professionals with responsibility over other personnel or projects should take the time to learn and hone the ability to be successful managers who are viewed as organizational leaders. Managers plan how tasks, projects, and normal operations will be accomplished within any applicable constraints such as budgetary restrictions, personnel capabilities, and any time deadlines. Planning is often followed by organizing any necessary resources and roles for the plan to function properly. Resources might include materials, personnel with specific capabilities, and finances. As mentioned earlier, all resources are generally limited so trade-offs between available resources are common. One popular saying, "Good, Quick, Cheap: choose which two you prefer," sums up the limitation on resources well. Goods or services sought that are of high quality (good) in a short amount of time (quick) will not typically be inexpensive (cheap). Inversely, if the same good or service is not needed quickly, it may be available at a reduced price and so with the combinations. The reason for this can be found in the organizing function of management. If a manager must schedule work to be done quickly, then something else will need to be put aside and worked on a later time, deliveries of materials cost more when they must be expedited, and quality suffers based on the effort made to make the good or service within specifications (the lower the required level of quality, the easier to produce). On the other hand, if there is no rush for the delivery of the goods or services, the cost is reduced because now the manager is able to schedule this work around other activities without any penalties. When managers staff their operations, they recruit, select, train, discipline, and reward employees. Performing this function well has a significant impact on the overall performance of the manager's area of responsibility. Poorly selected and trained employees can ensure the failure of a project. Managers must ensure that their employees are motivated to complete their work on time and to the desired degree of quality.

Directing work is quite possibly what most think of when they think of managers; someone telling others what to do and how to do it. However, there is a great deal more to it than just "barking" orders. Managers must learn to motivate employees, and there are nearly as many ways to do this as there are ways that people would prefer to be motivated. In addition, managers must also delegate some of their authority to others so that they may ensure subtasks are completed. It is important to remember that a leader may delegate authority but they may not delegate their responsibility. In other words, they may depend on others to complete specific tasks but they are ultimately responsible for the overall performance of the project or operation.

What then is controlling? Controlling is the process of ensuring that everything gets done according to the plan. Oversight of the work requires some tools for measuring performance and completion of individual tasks so that the plan is not unnecessarily disrupted. Performance metrics (or the measurement used) might include counts of completed products or parts, number of successful sales, tasks completed on time, and so on. It is essential to be certain that any metrics measure activity that matters to overall performance. There are some worthwhile software tools available to assist with management in general and project management specifically. Simply, web searches will identify such products as Microsoft Project that provides a tremendous amount of information and interactive capability. Other sources of information on various management topics include www.quickmba.com among others.

Management techniques have evolved considerably over the past decades. Possibly the first major step forward in formalizing management methodologies starts with the Scientific Management era most often associated with Taylor's "One Best Way." Taylor measured working activity and sought to optimize their movements and their tools. Many others were known during this time including the Galbraiths, on whom the original movie "Cheaper by the Dozen" was based, and who conducted time-motion analysis also to find the most efficient way of completing tasks. To this day, there exist charts for specific activities showing optimum time that assist planning production activities. Eventually, the Quality Movement came to pervade in management theory with Total Quality Management (TQM) as set forth initially in Japan by Dr. W. Edwards Demming during the reconstruction following Second World War. TQM moves management away from such strict numerical controls and more toward a cycle of continuous improvement and organizational pride in their products and services. Quite possibly, the most famous US company to embrace many of these concepts is Walmart. Newer additions to

the Quality Movement include Six Sigma and the Balanced Scorecard approaches. Six Sigma, named for its relation standard deviations (sigma) in a standard distribution (bell curve), seeks to reduce the number of defects. It is based on a system of specific employees that seek out defect-producing aspects of an operation and alter or enhance them to reduce the defects. The goal of Six Sigma is 3.4 defects per million incidences of production. Numerous texts are available as well as a considerable amount of free material online discussing management theories.

Functions and Functional Departments

Organizations of all sizes require several functions meant to assist overall performance by concentrating work effort within groups with the necessary skills. These may include accounting, HR, marketing, safety, security, sales, and production or operations. Specific functions often depend on the specific organization. However, some functions, like accounting, tend to be found in all organizations while others, like safety and security, may exist based on organization size or culture. Understanding at least a little about the purpose of a few of these departments offers an advantage in preparing proposals and obtaining necessary information.

The money management within any organization falls within the finance and accounting function. Strictly speaking, finance generally deals with what to do with money while the accounting function is focused on how much money there is, where it is, and where it is going. However, there are some fundamental concepts that make both work. Modern accounting used a double-entry method based on debits and credits made to specific accounts. An in-depth knowledge of this process is necessary in fraud investigations. In short, for every debit there is an equal credit. This process allows funds to be tracked with considerable detail. It is this detail that permits such careful measurement of an organization's operations. Accountants use reports of this information such as the statement of cash flows, profit and loss statement, and the balance sheet. The balance sheet shows at any one point in time the financial health of an organization in terms of current (short-term or less than 1 year) assets, long-term assets, and liabilities (monetary obligations to others). Because this information is based on objectively measurable activity, that is real transactions of money, and it is measured consistently using the same monetary unit (such as the US dollar or the euro), the assets and liabilities can be compared. Assets such as cash or account receivables (obligations from others to pay you) can be compared with liabilities (your financial obligations to others) using several ratios. These can be easily located through web searches of "accounting ratios" or "business ratios" to provide a better understanding of their use and value.

When presenting requests for funds and budgets, there is often an expected return on investment required by the organization. This is nothing more than a financial statement showing when an equipment purchase will add profit or value to the organization. The expected rate of return or hurdle rate and the return on investment may be calculated in three different ways: the Payback Method, the Individual Rate of Return, and Net Present Value. Each of these has advantages and shortcomings and each therefore is used at different times. The Payback Method is the simplest and measures the time it takes for the investment to be paid. The shortcoming here is the fact that future value is ignored but it is none the less a relatively easy calculation. For instance, an online reporting application for uniformed services officers with a cost of $10,000 that is meant to reduce the amount of paper and their need to deliver reports to the office would have a payback period of 5 years if it were to save $2,000 a year. It is an easy calculation; however, it neglects that the $2,000 savings continues each year afterward. For explanations of the Net Present Value and Individual Rate of Return methods run some web searches and play with some numbers.

Marketing and sales are the functions of trying to get customers to want your product or service instead of those offered by your competitors. Marketing functions with a more strategic point of view, while sales generally revolve around the one-on-one interaction necessary to actually close the deal. A marketing department will often conduct surveys to determine how the organization as a whole is perceived as well as its products or services are regarded by the public and its customer base. Consider your favorite television commercial. The marketing message will only be effective if you are able to remember the message and the product brand. It does little good for an organization to entertain the public if those viewers are unable to associate the

message with the organization. Effective marketing might include the Nike swoosh, the Microsoft Windows multicolored window pane, the Coca-Cola wave, and quite possibly the most notable of all is the McDonald's "M" just to mention a few. Each of the advertisements evokes an experience, a thought, and with any luck some brand loyalty in the customer. Consider this as it relates to security programs and security professionals. How many television shows have portrayed the "security guard" as overweight, slothful, wearing white socks with their dark uniform pants, carrying lots of keys, unobservant, and quick to surrender? Now how many have portrayed the officers that stayed at their post while the World Trade Center towers fell on September 11, 2001? Carefully marketing the security program to internal organizational partners paves the way for better relationships. Marketing messages are powerful, both positively and negatively, in affecting relationships. To ensure the right person receives the right message, marketing professionals create market segments that can be demographic, geographic, psychographic, or behavioristic. These segments allow the right message to be tailored to the right people. As an example, a sport utility vehicle can be marketed in a number of ways so it makes little sense to show it driving through snow to perspective customers in Florida when it can just as easily be shown driving along a beach or down a street devastated by a hurricane. Always remember, Right Message, Right Person, and Right Time for the best perception of a security program.

HR is the function name that has evolved from the personnel function within many organizations. HR professionals are typically concerned with the recruitment, selecting, hiring, discipline, compensation, and benefits for an organization's employees. The HR profession also has a recognized professional organization, the Society for Human Resources Management (SHRM) (www.shrm.org), with professional development opportunities and certifications for its members. The HR process requires considerable knowledge of federal and state employment law as well as organizational compliance with those laws. Issues of discrimination, compensation fairness, accommodation for disabled employees, workplace privacy are just a few that require the attention of the HR professional.

Asset Protection and Asset Protection Theory

Role of Asset Protection

Asset Protection, Loss Prevention, Resource Protection, and Security all describe essentially the same function, although there have been some heated debates about these titles. If management's function is to maximize the wealth or performance of an organization, then the security function is to preserve that capability from nonmarket-based threats. This too is open for debate and each organization must resolve what precisely the mission and role of the security function is rather than relying purely on an academic statement.

It has long been put forth that the security function fills its roll through the four Ds: Deter, Detect, Delay, and Deny. It is the goal to deter adversaries whenever possible, followed by detecting their intention to cause harm, then to delay their ability to cause that harm, and finally to deny them the ability to cause harm or to deny them the value of their efforts. Deterrence comes in forms such as training, awareness, barriers, and strong internal controls. Detection likewise may be found in electronic monitoring systems such as alarms and closed-circuit television (CCTV), audits, and aware personnel. Delays may be created by barriers, arguably by locks, security intervention, and most importantly multiple layers of protection also known as Defense-in-Depth. Denial might be the inktag at the retail store that destroys the stolen merchandise or the network "honeypot" that is used to trap and monitor the unwitting hacker.

Fundamental to the security professional is assessing security risks. Risk assessments permit the professional to determine what is being protected from what and then recommending how it will be protected. The risk assessment process, in short,

- identifies assets
- defines threats
- determines weaknesses and vulnerabilities
- establishes risks
- recommends countermeasures

It is imperative to know what is being protected first. These are the assets and this word should not be confused for the same term used by the accounting function. Assets may be tangible (physical) or intangible (nonphysical) such as reputation, trust, and goodwill. Knowing the value of these assets such as the financial and operational criticality to the organization provides perspective later when deciding on countermeasures. What then is endangering or threatening those assets? Is it vandals and petty thieves or skilled thieves, hackers, and natural disasters? Knowing what threats are most likely to occur permits the development of a security program that "fits" the organization's needs. Security has to exist for the sake of the organization not the other way around. This data may come from historical occurrences, anecdotal evidence from nearby organizations as well as similar organizations elsewhere in the world, and through scenario development. The latter method requires the security professional to take on an adversary's perspective. These threats should show which weaknesses within the organization may be exploited or where vulnerabilities exist. From this, the security professional should begin to determine the estimated risk of an actual manifestation of a threat and the potential consequences of a successfully completed attack. Finally, a series of countermeasures may be developed, considered in terms of cost versus benefit, and prioritized for recommendation to senior management. More information concerning this process may be found in articles available at www.ifpo.com, with other resources available through www.asisonline.org.

Why do people target individuals and organizations for crime and deviance? There are many theories on crime and crime causation discussed later in this chapter. Learning theories describing why deviance occurs is one step to seeking ways of disrupting that activity. There are arguments that location or setting can facilitate or deter crime as can be found in the research supporting the concepts of Defensible Space, Crime Prevention Through Environmental Design (CPTED), and Situational Crime Prevention. These techniques focus on altering the environment to deter deviance by making it less comfortable to do the wrong thing. Take for instance the concept of Natural Surveillance in which a person is less likely to commit some sort of deviant act if they believe they are being watched by others and that those watching them will take some sort of action, like calling for assistance. Again further information on these topics can be found through convenient web searches and in the article archives at www.ifpo.com.

Internal frauds occur when an employee, vendor, or anyone else with knowledge and access to organizational systems causes a loss. These are sometimes referred to as defalcations or the misappropriation, misuse, theft, or embezzlement of funds entrusted to the individual. One theory developed by Donald Cressey is the Fraud Triangle. Cressey argued that three conditions facilitated frauds:

- A perceived opportunity
- Rationalization
- Economic pressure

Here again, by recognizing causes of the act allows the security professional to develop ways of disrupting them before they begin. For instance, removing potential rationalizations for theft through regular awareness programs where employees are reminded that taking from the organization is theft. Another method may be offering access to consumer credit counseling to help remove economic pressures, or instituting strong controls supported by aggressive auditing to reduce perceived opportunities. For more information visit the IFPO article archives or the Association of Certified Fraud Examiners (www.acfe.com).

Risks are managed through risk management techniques. These broad techniques assist in the development of any protection planning and implementation of those plans. Risk management approaches include:

- Avoidance: eliminated the risk by removing the target altogether. For instance, many retailers no longer carry fur coats and accessories to avoid attacks by animal rights activists
- Reduction: reducing the risk of specific events through countermeasures
- Spreading: placing smaller amounts of the asset at multiple locations to limit the damage caused to asset as a whole at any one location

- Transfer—shifting responsibility for losses to other parties such as insurance companies or vendors
- Acceptance: accepting the risks and ultimately the consequences

Physical Security, Information Security, and Information Systems Security

While contemporary security is a relatively immature profession with its roots in Second World War, it existed for quite some time with a focus on physical security practices. Even in the protection of information, which for decades was stored entirely on paper or film, the focus remained on controlling physical access and the ability to copy the physical information. This all changed with the creation of the microprocessor, the computer, computer networks, and most importantly the Internet. This subset of the security industry, information systems security, has rapidly become a major focus. Now that information is stored almost entirely electronically, the ability to access, copy, and distribute it has changed in an equally dramatic way. The Cuckoo's Egg by Clifford Stohl is an excellent account of one of the first investigations against a dedicated hacker/cracker. Occurring in the 1980s, Stohl utilized a great deal of creativity and patience in an effort to track the movements of the hacker through the Lawrence Berkley National Laboratory computer system as well as many others throughout the United States.

The world of information technology and information system security has changed quite a bit since then. Most focus has been placed on the concepts of confidentiality, integrity, and availability (CIA). These tenets of information systems security can still be expanded on but nonetheless form a foundation. To be very brief, data must be made available to those authorized to access it and it must remain intact with any attempts at tampering being recorded. A rudimentary understanding of information systems security assists the security professional in speaking with all of their peers, physical security oriented, and information systems security oriented alike. Furthermore, even a limited understanding can go a long way to develop integrated protection programs that leverage the best of physical security programs and those of information systems.

Information networks are composed of hardware that transports data in the form of electronic signals. The Internet was developed through the Defense Advanced Research Projects Agency (DARPA) as a robust error correcting communications medium. To better understand networks and the Internet, picture an office building and think of the wires as hallways and the computers as offices. A visitor, in the form of data, comes in from the outside through the front door where a receptionist, or a security officer, assists the visitor. Just as the visitor requests access to the facility so does the data, except that instead of a receptionist the data, contained in packets, is intercepted by a firewall. A firewall is a physical device or software application meant to separate different networks, just as the front door and receptionist separates and directs visitors. At the receptionist desk, our visitor leaves an envelope for one of the employees in the building and the receptionist, after checking to be sure it is correctly addressed, sends it to the mailroom for sorting. The data packet, just like the envelope, is sent from the firewall to a router, which is a device that sends data to different areas of a network, its destination, or another router. Our sample envelope (data packet) is sent from the mailroom (router) to the receptionist of the intended department, here the receptionist acts as a router and sends it on to the intended recipient computer. Is there more to it? Absolutely, but the concept is a key to understand how the data moves. The Internet is a large number of interconnected networks. Data packets move through the Internet from router to router until they reach their destination, but there is a twist that gives the Internet redundancy and the ability to correct errors. Each packet openly displays its destination and as it reaches a router that router knows the next closest and fastest router to move the packet to its destination. This means that each packet that moves part of a message can travel along a unique path to its destination. Consequently, it is more difficult to interrupt an entire message. Further information may be found at the IFPO article archives, ASIS International (www.asisonline.org), the International Information Systems Security Certification Consortium (www.isc2.org), the SANS Institute (www.sans.org), and the Information Systems Security Association (www.issa.org).

Here then were a few key terms and concepts to consider while moving forward with professional development within the security industry. While no one organization could possibly provide all the information necessary to cover every aspect of the security industry, it is certainly possible for the dedicated individuals to continually strive to broaden their knowledge. This disciple of training creates a foundation from which to continuously improve as an individual professional and a culture for the individual's security department and program. The threats countered by an effective program are continuously changing, adapting, and improving. The adversary is not a static concept, so why then would a security professional think that their knowledge should be otherwise?

Questions

1. _____ provide the foundation for sharing written and spoken ideas.
2. Terms like _____, _____, _____, and rapport define the conduct of a security professional.
3. Security professionals must learn about organizations, their functional segments, and how they _____.
4. _____ of the organization permits the security professional to better mesh with other business professionals.
5. Governments obtain funds through the taxation of a population and businesses earn funds through _____.
6. A good or service is provided in exchange for _____.
7. Events and decisions within an organization affect _____ and groups.
8. _____ might include materials, personnel with specific capabilities, and finances.
9. When managers staff their operations they recruit, select, train, discipline, and _____ employees.
10. Managers may depend on others to complete specific tasks they are ultimately responsible for the overall performance of the _____ or _____.

4

Explaining Crime: Contemporary Criminological Theory

Whitney D. Gunter

Presently, there are dozens of criminological theories, hundreds of variations on the theories, and countless implications derived from each theory. Criminological theorists are on a never-ending mission to test and retest these theories; it is their professional life. Often the practical implications are not readily apparent and so practitioners of the criminal justice field may be considerably less interested in the scholarly theories discussed in journals. For this reason, the best place to begin this discussion is its purpose.

A scientific theory is a series of falsifiable statements about relationships between two or more observable phenomena. There are several parts of that definition that require further explanation. First, the statements of a theory are causal statements such as "X causes Y." Typically, crime is the latter part of these statements in criminological theories, while social factors often represent the former part. Additionally, all scientific theories relate to observable phenomena, meaning that theories involve things we know to exist, such as crime, rather than what we believe to exist, such as supernatural beings or luck. Finally, and perhaps most importantly, a theory's statements must be falsifiable. The scientific method requires that we can test the validity of statements. For example, "lack of parental attachment causes crime" is testable because we have ways to observe the degree of attachment a child has to his or her mother and father, whereas "life causes crime" and "demonic influences cause crime" are philosophical and religious statements that cannot be tested.

Ideally, a criminological theory will explain all four elements of crime, which are motivation, lack of controls/constraints (a freedom from social or internal pressure to behave in an approved manner), opportunity, and ability (see Table 4.1). Typically, it is too difficult to engage in rehabilitation to alter motivation, and lack of controls without government support and ability is just as tricky to remove (even impossible when ability constitutes knowledge instead of pragmatic abilities). Therefore, opportunity is of the greatest concern to individuals and small groups attempting to prevent crime.

Learning what causes crime is its own purpose to the theorists conducting research to develop and test these theories. However, the implications from theories represent a more practical reason for studying this complicated topic. By knowing what causes crime, it is possible to prevent it by removing its cause. These implications range from the relatively simple solutions (increasing punishment to deter, altering the environment to disrupt the process of the crime.) to the socially achievable (e.g., social programs to teach better parenting practices) to the radical implications (communism, socialism, etc.). For individuals in a managerial or supervisory position, the relatively simple solutions are the most feasible to implement and will be discussed in the greatest length in this chapter.

Table 4.1 The Four Parts of Crime

Parts of a Crime	Description
Motivation	A psychological drive that controls one's goals
Lack of constraint	The ability to rationalize one's actions or reject common beliefs when the crime goes against society's norms and rules
Opportunity	A situation in which it is possible to commit a crime (the right place and the right time).
Ability	Familiarity with the techniques of certain crimes. Especially necessary for complicated crimes like embezzlement

The Classical and Neoclassical Schools of Thought

Nonscientific theories of crime have likely existed since the dawn of civilization. Biblical and historical records can give us an idea of what these nonscientific theories constituted. In early times, someone who violated a law or rule of society was usually thought of as possessed or controlled by evil forces. These spiritual theories remained dominate or, at minimum, somewhat common in western civilization until roughly the early 20th century and still exist today in scientifically less advanced societies. Other nonscientific theories exist today through common beliefs and informal sources. These theories are known as folk theories and often are distorted or incomplete versions of scientific theories.

Scientific theories can similarly be split into categories. The oldest scientific criminological theory dates back to the 18th century and is the hallmark of the classical theories of crime.

General Deterrence

In 1764, Ceasare Beccaria published an essay called On Crimes and Punishments.[1] The essay was largely motivated by the politics of Beccaria's day as it gave specific outlines for the proper duties of legislature and judges in a demand for a fair and just system of punishment. Of greater interest to criminological theory's birth was Beccaria's description of what punishment ought to be. Beccaria based his statements about punishment on what we call today hedonistic psychology or hedonistic calculus, which assumes that humankind is rational (capable of thinking about consequences before acting) and makes calculated decisions based on a pleasure-seeking and pain-avoiding motivation.

Stealing is an excellent example of hedonistic calculus; an individual will be motivated to steal something because owning it would be more pleasurable than not. Buying the item would not be as pleasurable as stealing it because giving up the money required for the purchase would be a pain approximately equal to the pleasure gained from the item. Stealing, on the other hand, would only result in a loss if the perpetrator is caught and punished. Therefore, the best way to prevent a theft is to keep punishment more painful than the possible benefits of stealing.

So far, while this motivation is rarely discussed, it is fairly common sense for criminal justice practitioners. However, the way to maximize the effect of punishment is less clear and is where Beccaria's work is specific. Beccaria specified three goals for punishment: severity, celerity, and certainty.[2] For punishment to be an effective deterrent, all three goals must be

1 As cited in Vold, Bernard, and Snipes (2002).

2 As cited in Vold *et al.* (2002).

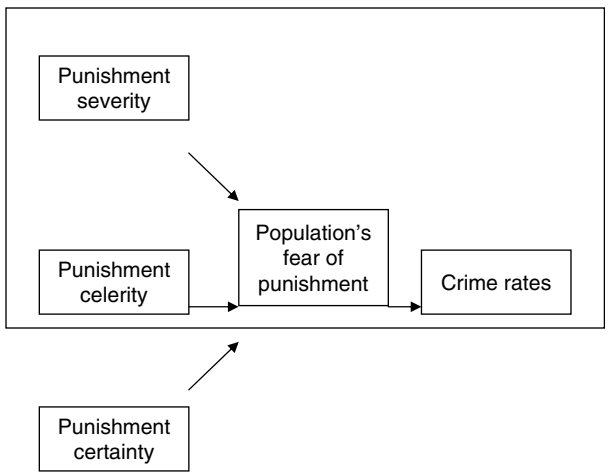
met. Certainty is, perhaps, the simplest of the three. It is based on the commonsense concept that the more likely punishment is, the more fearful the potential offender will be that he or she will be caught. The public spectacle of punishment is an element of certainty that is often overlooked in today's criminal justice system; if people do not witness or hear of the punishment, they will not fear it. Celerity, also referred to as swiftness and promptness, is best defined through the length of time that occurs between the crime and the punishment. The quicker a punishment occurs after the crime, the more obvious it will be to the public that the two events are clearly related. Severity is a concept common in the modern criminal justice system. It is often the element of deterrence most easily influenced through legislation and therefore becomes the target of "get tough on crime" policies. However, according to Beccaria's essay, severity only needs to exceed the amount of damage inflicted on society, "all beyond this is superfluous…."[3] In other words, punishment severity must be the amount necessary to make punishment more painful than the pleasure from the crime. Increasing severity once it has achieved this is no longer effective. Instead, certainty and celerity, while more difficult to increase, should become the focus for improving punishment's effectiveness in deterring crime.

It should be noted that two different deterrence theories are derived from Beccaria's work.[4] The general deterrence theory focuses on the public's willingness to commit crimes after witnessing or hearing of the punishment of an already existing criminal (see Figure 4.2). Specific deterrence theory, conversely, discusses the effects of punishment on the individual being punished (see Figure 4.3). It uses many of the same principles as general deterrence theory. The corrections system currently used in the United States gives a great example of both forms of deterrence. First, it creates a specific deterrence because (in theory) convicts do not enjoy their stay in prison and will not want to take actions that could result in another prison sentence. Second, citizens are aware of the unpleasantness of prisons and also wish to avoid spending time behind bars, thus creating a general deterrence. It should be noted, though, that Beccaria would place a greater emphasis on having a public spectacle in punishment, such as in public executions or punishments including humiliation.

Rational Choice Perspective

The classical theory of deterrence is a relatively simple model that often fails to explain all the elements of crime and criminality. Though no theory has perfected a formula for explaining all

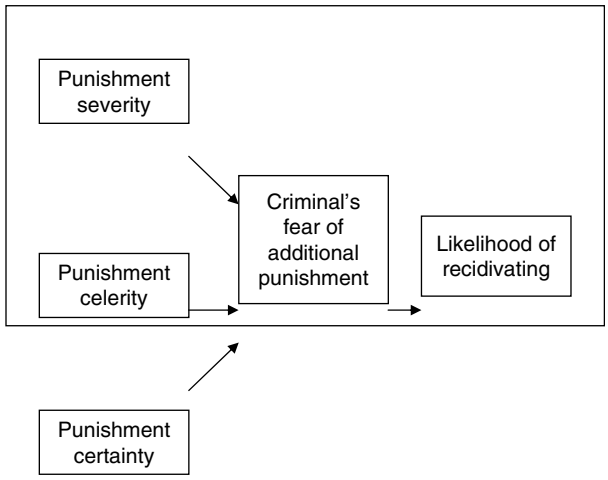
FIGURE 4.2 General Deterrence Theory



3 As cited in Vold *et al.* (2002, p. 18).

4 As cited in Vold *et al.* (2002).

FIGURE 4.3 Specific Deterrence Theory



the variance, the rational choice perspective is a clear step forward from Beccaria's work and with it began the neoclassical, sometimes called neuve classical, school of criminology.

Rational choice has existed in various forms throughout the last few decades. The earliest version usually identified is Becker's economic approach to crime from the late 1960s.[5] However, the most often studied rational choice theory, and the one discussed here, was developed in 1985 by Clark and Cornish. The theory begins with the assumption that there is a purpose behind every crime (obviously to the benefit of the offender). Further, the criminal chooses to commit the crime based on his limited ability to weigh the benefits and risks involved. The term limited was specifically chosen to describe the criminal's ability to reason not because of some mental deficiency on the part the offender, but rather because there is no way for a single person to know all the potential benefits and risks involved. Essentially, potential offenders always face uncertainty and therefore do not always make the best decisions.

The rational choice model includes three parts: initiation (leading up to the first offense), habituation (continued offending), and desistance (either becoming noncriminal or moving to a different crime).[6] Focusing on each of these divisions is not practical for the topic of asset protection, but some of the variables provided in the model are of use. The variables include background factors (e.g., upbringing), current life circumstances (e.g., unemployed), and situational variables. The situational variables are of most interest here as they are the most easily influenced by individuals outside of the potential offender's personal life such as a security officer. For a better look at these situational variables, routine activities theory provides a more in-depth focus on opportunity.

Routine Activity

Routine activity theory was created in 1979 by Cohen and Felson. Unlike most theories, both classical and contemporary, routine activity theory focuses not on why people want to commit crimes, but rather why crimes occur at specific places and times. This theory will be quite familiar to professionals in asset protection as it is one of the more practical theories and is compatible with common practices of the profession (target hardening, CPTED, Situational Crime Prevention, etc.). Rather than focus on crime from the criminal's perspective, this theory places higher emphasis on what leads to victimization.

The main posit of Cohen and Felson's routine activity theory is that crime is the function of a space-time convergence of a motivated offender, a suitable target, and a lack of capable

5 Paternoster and Bachman (2001).

6 Clark and Cornish (1985).

guardianship.[7] In other words, a crime (theft) occurs when someone interested in stealing notices that an accessible target is not being guarded. The authors' interest in the theory stems from an attempt to explain increased crime rates in the modern world. Specifically, an increase in property crime is the result of greater availability of targets and increased absence of guardianship. The original article primarily focused on family households to explain this change. In short, the modern world has left the family less likely to be home, while simultaneously increasing the amount of valuables kept inside the home.

In the time since the theory originated, routine activity theory has been used to empirically describe and test many practices already in place in the asset protection profession. The guardianship variable has received much attention in subsequent research. Research has described capable guardians as police officers, security officers, store employees, or any person capable of defending his or her property. In addition, research has extended the original concept of guardianship to include nonhuman guardians, such as security cameras and alarm systems, as they would increase the likelihood of a capable guardian arriving should a crime occur. The quality of guardianship can also be a consideration based on appearance of professionalism, physical stature or the any interactive CCTV capabilities, and ability to summon assistance quickly.

The suitable target is also a concept used for practical application of the theory. Research on routine activity theory has described the suitability of a target in numerous ways. However, most agree that the financial value, inertia (ease in moving the item), accessibility, and visibility of the target are all related to suitability in one way or another. The practical implication from this is target hardening, which varies based on each target's usefulness. For example, an item for sale should be accessible and visible for the benefit of customers. Doing so makes it inherently vulnerable to theft. Options might include attaching the item to the counter to prevent removal with "live" merchandise secured separately that sales associates may access, thus reducing the potential inertia of the item and increasing the guardianship of the live merchandise without truly reducing accessibility. In other situations, such as the counting of money in a vault, it may not be possible to change the accessibility or inertia. Instead the level of guardianship is significantly increased with all activity conducted by two persons (dual control), while monitored and recorded by CCTV, and all funds counted prior to the departure of the involved employees.

The Positivist School of Thought

Unlike the theories of the classical school of thought, which often assume that everyone is equally likely to become a criminal and it is the situation before them that causes them to choose to be criminal, positivist theory focuses more on why some people are more prone to criminality than others. It should be noted that while the positivist school of thought has undoubtedly received more attention over the last century, it is not necessarily more important than the classical school. Most experts would agree that both a potential criminal's personality and the situation before him or her play a role in creating crime. What is debatable is which plays the bigger role.

The positivist school of thought is often credited to Cesare Lombroso, whose book (*The Criminal Man*) is often cited as the earliest positivist theory.[8] Lombroso's main hypothesis was that criminals are atavistic, an evolutionary throwback to primitive man. Further, the criminals Lombroso described had five or more physical abnormalities (large nose, large skull, increased body hair, etc.) and were the "born criminal." While the theory has since been widely ridiculed for being overly simplistic and discriminatory against non-Italians (and even against groups of Italians from certain areas of Italy), it was still one of the first to go beyond describing criminality as a choice or a result of demonic activity.

Today, most positivist theories focus on various social factors that affect one's willingness to commit crime, but biology and psychology are also present. These theories are often more elaborate and, similarly, offer complex solutions. As such, the conclusions are normally less practical for one person or business to implement. For this reason, these theories will

7 Cohen and Felson (1979).

8 Vold *et al.* (2002).

receive less attention in this chapter. However, interested readers would do well to learn more about these complex theories using any one of the various sources referenced.

Social Disorganization

One of the oldest positivist theories still researched today, social disorganization was the product of research in the 1920s by Clifford R. Shaw and Henry D. McKay.[9] The research primarily focused on the city of Chicago and the "concentric zones" that existed there. As a city slowly expands outward, each circular zone also expands by invading the next zone. While each zone has individual characteristics, the ones essential to social disorganization are the first and second zones. The first zone, the business district, is located in the center of the city and the second zone, the area with the poorest residents, exists around the first. The second zone is uniquely plagued with a series of invasions by both new immigrants and the expanding business district. The areas most affected by this change are called the interstitial zone. The rapid change creates social disorganization, which allows crime to occur.

More recent iterations of the theory are more representative of present-day cities. Sampson's social disorganization theory, collective efficacy,[10] is the version most commonly used in current research. The focus in Sampson's theory is on zones of transition in inner-city areas. People in these areas have high "residential mobility," which means they can easily move, yet they usually move to other zones of transition. In essence, these people are stuck in poor areas, but still move often. This creates a lack of collective efficacy because frequently moving residents cannot have mutual trust with neighbors. In other words, residents of inner cities don't get to know their neighbors. This combined with other factors, such as structural disadvantage, explains the higher crime rates in certain areas of cities.

Social Learning Theories

Social learning theory, another long-studied theory, was developed and published in various stages between 1934 and 1947. Differential association, as the first social learning theory was later dubbed, was the work of Edwin Sutherland and, to a lesser extent, his coauthor, Donald Cressey. The main hypothesis of differential association is that criminal behavior is learned. More specifically, "a person becomes delinquent because of an excess of definitions favorable to violation of law over definitions unfavorable to violation of law."[11] In more common language, a person becomes criminal when the majority, rather than a minority, of their friends and family are criminal or otherwise in favor of ignoring the law. While the theory and subsequent research goes beyond simply the number of criminals versus noncriminals (focusing on the frequency, duration, priority, and intensity of procriminal messages from friends and family), the main hypothesis nonetheless is that criminal behavior is learned from other people. Further, people must learn three things from criminals to become criminal themselves, which include motives, attitudes (a rationalization for breaking the law), and techniques (skills for certain crimes).

Social learning theories, however, are not limited to differential association. Rather, more contemporary social learning theories have expanded on Sutherland's work, spawning many variations. One of the more often cited social learning theories, from Burgess and Akers in 1966, includes more societal level concepts to explain how society as a whole contributes to delinquency and criminality as well. For example, differential reinforcement explains how potential rewards and punishments that follow crimes can influence the potential offender and recidivists.

Techniques of Neutralization

Sometimes called drift theory, the techniques of neutralization are used to explain how people, especially delinquents, can believe a crime is wrong, commit the crime, and still go on believing

9 Shaw and McKay (1942).

10 Sampson and Groves (1989).

11 Sutherland and Cressey (1960/2003, p. 132).

the crime is wrong. In other words, the techniques of neutralization are ways for offenders to rationalize their actions and essentially create an exception specifically tailored for their own actions. Table 4.4 explains each of the techniques and example usages.[12]

Strain Theories

While strain theories date back to Durkheim, criminological theories using strain are more recent, relatively speaking. The first strain theory of crime, sometimes called "anomie" (not to be confused with Durkheim's concept on which this theory is based), was developed by Robert Merton in 1938. According to it, Americans share two distinct beliefs. First, they want "the American dream." That is, people want to be successful financially and live a middle or upper-class life. Second, Americans live by a puritan work ethic. They believe hard work is the only way to become successful. Most of the time, people are conformists and achieve their goals using their work ethic. When people experience strain, which is a disjunction between their goals and means, meaning they can't get what they want doing what they believe is right, they must respond in one of the four ways. First, they can innovate by rejecting the traditional means (stealing or other profitable crimes). Second, they can turn to ritualism (keep working hard, even though they know it won't help). Third, they can become retreatists and turn to drugs. Finally, they can rebel and create new goals and means (typically rejecting capitalism altogether, sometimes forming microsocieties like communes) (Table 4.5).

The next strain theory came nearly 20 years later in 1955 when Albert Cohen published his strain theory, sometimes called status frustration. One of the major differences between Cohen's theory and others is his assumption of goals, which he describes as status rather than financial. According to Cohen, the public school system is designed for middle-class children. When lower-class children fail because teachers use a "middle-class measuring rod," they are humiliated, and cannot achieve status among their peers. In response, the children seek status from other sources. Delinquent gangs are the preferable source of status for many of these youths and result in children committing crimes to gain approval from other delinquent peers.

Table 4.4 Techniques of Neutralization

Techniques of Neutralization	Sample Usage
Denial of responsibility	It was an accident. It wasn't my fault
Denial of injury	It didn't hurt anyone. I was just borrowing it
Denial of victim	He deserved it. His kind deserve it
Condemnation of the condemners	The police are corrupt. That teacher plays favorites anyway. He would have done it too
Appeals to higher loyalties	I was just following orders. I was doing God's work

Table 4.5 Possible Outcomes of Strain

	Goal	Mean
Conformity	+	+
Innovation	+	–
Ritualism	–	+
Retreatism	–	–
Rebellion	+/–	+/–

12 Sykes and Matza (1957).

Another classic strain theory is differential opportunity from Cloward and Ohlin in 1960. Similar to the previous theories, Cloward and Ohlin believed that some youth fail to obtain the goals they want and look for alternatives. What alternative they choose, much like Merton's theory, vary. If illegitimate means for obtaining money exists (e.g., organized crime, fencing opportunities, etc.) and the youth has the skill necessary, he will join a "criminal" gang. If these opportunities don't exist, on the other hand, the youth may turn to a "conflict" gang that acts out in violence. Finally, if the youth fails in both criminal and conflict gangs, or if these types of gangs are incompatible with the youth's morality, a "retreatist subculture" involving drugs is a last resort for "double failures."

The most recent reiteration of strain theory, general strain theory, came in 1992 from Robert Agnew. The flexibility and generality of the theory is both its strength and weakness. According to the theory, strain can be caused by one of two actions: the removal of positively valued stimuli or the presentation of negative stimuli. Essentially, people commit crimes when they lose something they like or when someone does something to them they do not like. This theory has been praised for its broadness, but has also been criticized for not being specific enough. Current research is investigating which negative and positive stimuli have more powerful effects on crime.

Control Theories

Unlike most criminological theories, which focus on why someone becomes criminal, control theories focus on why some people don't become criminals. In essence, control theories examine the parts of society that act to prevent criminality. In some cases, this can involve the social ramifications of crime, but usually the factors studied are nonfinancial.

While not the oldest control theory, Travis Hirschi's (1969) theory of social bonding is probably the most often discussed control theory. According to it, there are four social factors that prevent delinquency: attachment, commitment, involvement, and belief. The first, attachment, refers to one's affection for his or her parents and school. The greater one's attachment is, the more likely one is to care about the disapproval that would result from criminality. The second element, commitment, is similar to classical theories in its focus on the negative results of crime. When someone has made an investment that would be lost due to crime, a "stake in conformity," that person is less likely to risk losing said investment. Unlike the classical theories, however, Hirschi allowed for this investment to be more than just money or freedom. The commitment can also include a career that could be lost or a marriage that could be ruined.

The third concept that affects a social bond is involvement, which can include employment or other time-consuming activities. For involvement, the idea is not that these activities produce prosocial attitudes, but rather that a potential criminal without free time will not have the opportunity to commit a crime. Finally, the belief element is fairly obvious; the belief that something is wrong will prevent the believer from turning to crime. Worthy of note in this theory, however, is that Hirschi posited that we live in a consensus-based society, meaning that everyone holds similar beliefs. What differs from person to person is the strength of the belief; the weaker the belief, the more willing someone is to act against their own belief.

Another control theory that should be addressed is the low self-control theory by Gottfredson and Hirschi (1990). It takes the elements discussed in both Hirschi's earlier theory and other positivist theories, and further investigates what causes them. The main hypothesis is that poor child rearing is the root cause of all crime, as it results in low self-control. Additionally, they state that most or all of one's self-control is established before the age of eight and remains constant throughout one's life.

It should be noted that low self-control is currently one of the most heavily debated theories. There is currently a divide between theorists supportive of it, who believe it explains why a minority of people account for the majority of crime, and theorists who claim that it fails to explain why most offending occurs during the teenage years if low self-control remains after that time.

Other Explanations of Criminality

For the most part, the theories discussed so far are rooted in a consensus paradigm, which makes an assumption that crime is a deviant act that goes against society's beliefs. Conversely, a conflict

paradigm theory explains crime as a normal function of certain groups. Theories within this paradigm are often called theories of critical criminology. The groups in these theories, however, have neither the power to create laws protecting their preferred actions nor the ability to remove laws baring such actions. For example, a critical theory could explain violent behavior as a legitimate source of status for certain subcultures. White-collar crime is one of the major strengths of conflict theories, as the lack of focus on white-collar crimes in society is explained because people with power, who decide which laws to enforce, are usually the perpetrators of such crimes.

Sometimes considered a critical theory and other times listed separately, Marxist theories also explain crime differently than consensus theories. The major characteristic of Marxist theories that separates them from other critical theories, other than stemming from Karl Marx's works, is the focus on economic class. Unlike other conflict theories, which are more general in defining the groups involved, Marxist theories specify that the conflict is between the bourgeois upper class and the proletarian working class. According to the theories, the bourgeois own and control the means of production (businesses, factories, etc.) and keep all the money their workers earn, sans their paychecks which only gives them enough to buy food and other necessities to stay alive and healthy enough to work. More specific to crime, this greed by the capitalists creates a society in which everyone is selfish and uncaring, which leads to a willingness to commit crimes. The ultimate solution, of course, is almost always the rejection of capitalism in favor of a socialist society (though not necessarily communism).

Not all of the alternative explanations of crime are at odds with the consensus theories. In some cases, special theories exist for certain situations that are frequently compatible with a consensus perspective. Feminist criminological theories, for example, can explain why female delinquency is increasing (equal treatment), but still has not reached the prevalence of delinquency by males. They also explain why females are less likely in general to commit crimes. These explanations sometimes focus on physical differences (hormonal aggression, strength, etc.), but often focus on social trends and the differential treatment of girls and boys during childhood (being taught to be passive rather than aggressive). Similarly, life course theories explain why teenage youth account for the majority of crime. These theories usually involve explaining the criminal tendencies as a function of the transition from childhood to adulthood due to the increased freedom without adult obligations (work, marriage, parenting, etc.).

Criminological Theories in the Real World

The criminological theories of today theoretically explain crime rather well. In the theories, X causes Y and sometimes Y_1 causes Y_2 too. Everything adds up and nothing goes unexplained. However, in the statistical analyses used to test the theories, there is a term that is a significant challenge to the theories: the error term.

As you may recall, a theory is a series of falsifiable statements about relationships between two or more observable phenomena. Because true scientific theories are inherently falsifiable, they can and should be tested to determine their validity and reliability. When a theory is tested with real-world data, usually using survey data, a lot of crime goes unexplained. Using current statistical techniques, such as regression models using multiple controls or structural equation modeling (see Table 4.6), a theory is generally considered a success if it can explain 10–20% of the variation in crime. Essentially, each theory explains only a small portion of crime. Even more elaborate models that combine theories, often called integrated theories, can't explain everything. There are other obstacles as well. For example, researchers almost always find that delinquents are more likely than nondelinquents to report that their friends are also delinquent. While this would be considered support for social learning theories, does it really prove anything? It could mean that delinquency is learned, but it could also mean that delinquents exaggerate their friends' criminality on surveys or it could simply be proving that delinquents find other delinquents for friends.

Presently, theories find moderate support in empirical tests. While no theory has been proven to be completely true, nearly all discussed here are true enough to be better than no theory at all. For example, Hirschi's social bond theory often receives support when testing attachment and commitment. Involvement, however, often results in insignificant findings (usually explained by the relatively short amount of time needed to commit a crime).

Table 4.6 Common Statistical Procedures

Procedure	Description
t-Test	Compares groups to see if there are significant differences. Example usage: to see if people who have read a procrime essay believe crime is more acceptable than those who have not read the essay
Regression	Determines how much variance in a dependent variable (e.g., crime) is caused by changes in other measured variables. Example outcome: "attachment was the most powerful predictor of delinquency"
Structural equation modeling (SEM)	Similar to regression, but allows for more complex models that include multiple paths of causality. Example: A causes B, and B and C both cause Y. Explains and measures mediating effects
Hierarchical linear modeling (HLM)	Controls for "nesting effects" in certain sampling techniques that result in multiple classes or other clusters being sampled. In other words, determines whether changes are due to individual differences, classroom level variables, school characteristics, or geographic region

In the simplest of terms, criminological theories are far from perfect. There is still much to be explained and the theories we do have are each only small pieces of a very large puzzle, but knowing the basics is the first step to explaining the phenomenon of crime.

References

R. Agnew (1992). Foundation for a general strain theory of crime and delinquency. *Criminology* 30:47–87.

R. L. Burgess and R. L. Akers (1966). A differential association-reinforcement theory of criminal behavior. *Social Problems* 14:128–147.

R. V. Clarke and D. B. Cornish (2001). Rational choice. In *Explaining Criminals and Crime: Essays in Contemporary Criminological Theory*, eds. R. Paternoster and R. Bachman. Los Angeles, CA: Roxbury, pp. 23–42.

R. A. Cloward and L. F. Ohlin (1960). *Delinquency and Opportunity: A Theory of Delinquent Gangs*. New York, NY: Free Press.

A. K. Cohen (1955). *Delinquent Boys: The Culture of the Gang*. Glencoe, IL: Free Press.

L. E. Cohen and M. Felson (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review* 44:588–608.

M. R. Gottfredson and T. Hirschi (1990). *A General Theory of Crime*. Stanford, CA: Stanford University.

T. Hirschi (1969). *The Causes of Delinquency*. Berkeley, CA: University of California.

R. K. Merton (1938). Social structure and anomie. *American Sociological Review* 3.

R. Paternoster and R. Bachman (2001). *Explaining Criminals and Crime: Essays in Contemporary Criminological Theory*. Los Angeles, CA: Roxbury.

R. J. Sampson and W. B. Groves (1989). Community structure and crime: Testing social-disorganization theory. *American Journal of Sociology* 94:774–802.

C. R. Shaw and H. D. McKay (1942). *Juvenile Delinquency and Urban Areas*. Chicago, IL: University of Chicago.
E. H. Sutherland and D. R. Cressey (2003). A theory of differential association. In *Criminological Theory: Past to Present: Essential Readings*, eds. F. T. Cullen and R. Agnew, 2nd edn. Los Angeles, CA: Roxbury, pp. 131–134. (Reprinted from Principles of criminology, 6th edn., 1960.)
G. M. Sykes and D. Matza (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review* 22:664–670.
G. B. Vold, T. J. Bernard, and J. B. Snipes (2002). *Theoretical Criminology*, 5th edn. New York, NY: Oxford.

Appendix: Quick Reference Theory Matrix

Theory	Description
Deterrence Beccaria (1764)	When punishment severity, celerity, and certainty are low, people will commit crimes because the punishment is less likely and less significant
Rational choice Clark and Cornish (1985)	People commit crimes because they believe it to be an easier and more beneficial option
Routine activity Cohen/Felson (1979)	A crime occurs when a motivated offender and suitable target meet in time and space if a capable guardian is not present
Social disorganization Shaw/McKay; Sampson and Groves (1920s; 1980s)	Crime occurs in areas where frequent moving occurs and where the city lack collective efficacy to enforce laws and promote other social programs
Social learning theory Sutherland/Cressey; Burgess and Akers 1947; 1966	Crime is learned through social interaction with criminals and people supportive of crime. The motive, attitudes, and techniques supportive of crime are transmitted primarily from family and friends. Society as a whole also contributes through rewards/punishments
Techniques of neutralization Sykes and Matza (1957)	Explains how people with conforming beliefs can rationalize their actions through denial and shifting the blame
Strain Merton; Cohen; Cloward and Ohlin (1950s)	People turn to crime (for differing reasons depending on the theorist) when their chance of achieving their goal through convention means is blocked. Usually focuses on the lower class being blocked unintentionally by the middle class
General strain Agnew (1992)	Crime is the result of the removal of positively valued stimuli or the presentation of negative stimuli.
Social bond Hirschi (1969)	Crime is prevented when a potential delinquent has attachment to parents or school, commitment to a convention way of life, involvement in noncriminal activities, and/or strong beliefs

(Continued)

Theory	Description
Low self-control Gottfredson and Hirschi (1990)	Crime is prevented when someone has high self-control. People with low self-control are present-oriented and do not see future consequences. Poor childrearing causes low self-control
Conflict/critical theories	The people in power use their power by creating laws that keep others, usually minorities or the lower class, in check
Marxist theories	Similar to conflict, but specifies that the
Theory	Description
	parties involved are the bourgeois upper class and the proletarian working class and that crime is the result of continued greed and selfishness
Feminist theories	Theories that explain why female delinquency is increasing and why females are less likely in general to commit crimes
Life-course theories	Theories that explain why teenage youth account for the majority of crime

Quiz

1. Which of the following is not true of a scientific theory?
   a) It must be falsifiable
   b) It must be about observable phenomena
   c) It must be a proven fact
   d) It must describe relationships
2. Motivation and opportunity serve as the two halves of a crime. ☐ T ☐ F
3. Which of the following statements best describes the difference between general and specific deterrence?
   a) Specific deterrence is about a specific crime
   b) Specific deterrence is more specific in nature
   c) Specific deterrence is targeted at a specific individual
   d) Specific deterrence has never been used in practice
4. In the neoclassical school, which of the following assumptions is not made about individuals?
   a) They are logical
   b) They are demonically possessed
   c) They are hedonistic motivated
   d) They can choose to commit a crime
5. Which of the following statements is most likely to be associated with the positivist school of thought?
   a) Everyone is the same
   b) Crime is best prevented through deterrence
   c) The logistics of crime precede all else
   d) People are a product of their environment

6. Which type of theory places an emphasis on why people *don't* become criminals?
   a) Control theories
   b) Classical theories
   c) Positivist theories
   d) Marxist theories

7. According to early strain theory, which of the following describes crime used to make money?
   a) Conformity
   b) Innovation
   c) Retreatism
   d) Ritualism

8. According to the techniques of neutralization, claiming one's victim deserved being victimized is an example of which technique?
   a) Denial of injury
   b) Denial of victim
   c) Appeals to higher loyalties
   d) Condemnation of the condemners

9. Feminist theories of crime always seek to explain why men are abusive. ☐ T ☐ F

10. Which of the following statements about theories is not true?
    a) Criminological theory cannot currently explain all crime
    b) Most criminological theories explain a small to modest amount of variation
    c) Most criminological theories have no policy implications whatsoever
    d) A few theories are incompatible, but most could potentially be integrated

This page intentionally left blank

UNIT II

Human Resource Management

This page intentionally left blank

1

Recruitment and Retention of Security Personnel: Understanding and Meeting the Challenge

Christopher A. Hertig, Bryan Kling, and Michael Dannecker

Introduction

Recruitment is where marketing of the organization and employee selection merge. It is, ideally, a marriage of the two processes. An inherent difficulty with recruitment is that the process is initiated only when there is a need to hire new personnel. The recruitment effort at this point is behind schedule. While an organization cannot advertise job openings it doesn't have, not starting the process until after vacancies occur means the employer is playing "catch-up ball." A recruitment process whereby the employing organization is continuously reaching out to potential applicants would seem to be the ideal situation. The artful marriage of personnel recruitment to a marketing campaign may provide this.

Within the security industry such an arrangement must take place in both the macro- and microemployment environments. Potential applicants must be aware of job and career potential as protection officers, loss prevention agents, investigators, supervisors, and directors. They must then know about specific job openings in particular organizations. There is some degree of overlap between macro- and microrecruiting efforts.

> *The securing and training of proper persons is at the root of efficiency.*
> —Sir Robert Peel

Contemporary protection forces should take note of the above statement, which is commonly attributed to Sir Robert Peel. Selection starts with recruitment. Targeting a specific type of individual and approaching those individuals through the appropriate channels will help ensure that the new employee fits the job demands.

Traditional recruitment methods may not meet the demands of the future for those organizations wishing to hire security personnel. The labor pool may be shrinking because of demographic trends. The retirement of "baby boomers" is one factor negatively affecting retention. Recruitment may be hurt by fewer persons entering the job market. Demographics trends reveal a decrease in the number of high school graduates in the United States for the years 2007–2112. This change will be more pronounced in some areas than in others such as Western Pennsylvania, which will see a more marked drop than will the rest of the nation (Mussano, 2006). This ties in with the traditional vagaries of labor markets which vary significantly by geographic area. So too do the expectations of succeeding generations of employees. Finally, increased job demands in terms of technical expertise (computerized detection equipment, access control and surveillance systems, etc.) and public expectation (customer

Table 1.1 Knowledge, Skills, and Abilities Expected of Security Personnel

Technical Expertise	Public Expectation
Detection equipment (EAS, X-ray, metal detectors, explosive detectors, etc.)	Counterterrorism role involving knowledge of terrorism, prevention, and response
Access control systems including readers, monitors, and locking systems	Customer service role where there is an appreciation of marketing as well as public relations
Surveillance systems including cameras, transmission method, monitors, and recorders	Emergency response functions for terrorism, assaultive behavior, fires, labor disturbances, and natural disasters

service role, counterterrorism role, and emergency response functions) require a new look at what type of person is needed and how best to attract and retain that person. Table 1.1 is a simplified "menu" of knowledge, skill, and ability areas. Specific job task analyses reveal considerably more detail.

In addition to these competencies, there is the necessity for in-depth knowledge and appreciation of the environment the officers are protecting. Effective socialization to the employer culture can be the difference between a present but isolated security function and an integrated, fully effective addition to an organization. This includes organizational structure, funding sources, operations, and culture. They must understand the retail business or the school administrative structure or the nonprofit nature of the church.

Some appreciable time and effort must be spent in orientation. The orientation process should include exposure to all aspects of organizational operations. In addition to these "happy side" effects of socialization, this broad knowledge prepares the security officer to be in a position to recognize incorrect or unauthorized situations in respect to normal operations.

Recruitment

Recruitment efforts begin after a decision has been made to add to present staffing levels. This can occur because of

1. An expansion of the need for personnel. This is generally the adding of additional line employees. It may, however, be the acquisition of supervisory, staff, or managerial personnel. It may be temporary or permanent in nature. It can even encompass staffing operations that are new or creating entirely new positions.
2. Replacement of personnel who have departed. This may be caused by retirement, promotion or regular attrition.

The next phase is to identify the ideal job candidate. This involves conducting a detailed job task analysis. All essential functions of the job must be identified. Typically, the Human Resource (HR) department of the organization will have a current job description on file and available for the position. This job description should be obtained and consulted regarding specific requirements of the position to be filled. The security functions of any organization are shaped by the needs of the larger entity. For example, because of the size and configuration of the facility or business operation, the security officer candidate may be required to walk long distances, climb ladders, or operate complex computer and CCTV systems. These various features of the job will dictate the specific physical and mental requirements of the candidate.

Job duties should then be assessed in terms of the cultural fit that is expected of the new employee. After the "what" of the job has been laid out, it then becomes necessary to describe the "how" of the job.

Internal Recruitment

An employer's most valuable asset should be its employees. There is no better place to recruit for your company than from within. This internal recruitment can take on many facets: promotion, upsizing, downsizing, etc. There are several ways employers can recruit from within.

Bulletin: The simplest form of a job posting is the bulletin. Having an HR area where job/promotional opportunities exist can be a means for this bulletin to be displayed. A bulletin board of sorts can accomplish this need. These boards can be placed in areas such as employee cafeterias, rest area, and training rooms.

Interoffice mail: Sending all employees a memo or bulletin is another way to recruit internally.

Electronic: If the employer is a mid- to larger-size organization, it can use an "Intranet" to post job openings/promotion opportunities. The intranet allows all employees access to this information. Additionally, it will allow employers to thwart off any innuendo of hiding open positions. The same can be accomplished by use of an internal e-mailing system. In-house blogs may also be used.

Relational: During the course of normal interaction of security officers and other employees, the alert and friendly security officer typically forges sociable relationships with employees from all functions of the organization. This interaction provides an excellent recruitment opportunity for current and future job openings on the security team.

Skills inventories: These can be maintained so that when a particular competency is required the employees possessing it can be quickly recruited. It may be both enlightening and useful to maintain a skills inventory for operational purposes in addition to its utility in recruitment efforts. Security departments often have a wide array of individuals with unique skills. This knowledge can aid in daily and emergency operations. It can also be used to enhance the image of the security department within the parent or client organization.

External Recruitment

Newspaper ads: These have traditionally been used to recruit personnel over a wide area in a rapid manner. Newspaper ads may tend to reach those persons who are currently unemployed. In many cases, this is not the optimal target group.

Newspaper ads should be seen as "ads." They are representations of the organization to a large segment of the general public. Within the general public are potential employees, clients, and customers. This recruitment tool may take longer to bear fruit than other electronic, immediate options due to print cycle and distribution limits.

Web site advertising: It has the advantage of being "24/7" at low cost. Contemporary newspaper ads often have Web sites so that two distinct audiences are reached. Another development is the use of Web sites for advertising jobs; for example, through Lpjobs.com and the Career Center on the Web site of the International Foundation for Protection Officers. LPJobs.com is sponsored by the *Loss Prevention* magazine and lists jobs in retail loss prevention throughout the United States. Listings are for LP personnel at all levels. The National Association of Security Companies also has a Web site job center for contract security officers.

The use of Web sites for recruiting will only increase over time. Unfortunately, if potential applicants are unaware of the existence of the employer or industry, they will not be as effective as they could be. Outreach efforts by professional organizations such as ASIS and the Partnership for Careers in Law, Public Safety, Corrections and Security are essential.

Microefforts by employers will use Web sites. These give a continuous advertisement about the employing organization at a fixed cost. Effective programs will have attractive sites that convey the culture and values of the employer. They will also be linked to other sites. Contract service firms who are members of the National Association of Security Companies may use their site, etc.

Employee referral bonus programs: These programs offer incentives to employees to seek out prospective employees. Most programs offer monetary compensation and there are guidelines. These guidelines usually state that the new employees found must stay with

the organization for a set amount of time. Benefits are twofold. The organization gains an employee who is more likely to want to be employed. The employee who recruited the new person gets compensated and will be working with someone he or she feels is competent and knowledgeable.

Referrals are a good way to obtain applicants as model employees are perhaps best prepared to find persons with characteristics similar to their own. Referrals can be done informally. Various methods of gaining referrals can be employed, such as developing a horizontal promotion scheme where certain designated persons are recruiters. Employee referral programs tend to wane over time (Berkshire, 2005).

Bonuses may plateau over time with the numbers of personnel being recruited remaining stable. In some cases there may even be a drop in new hires. In order to revitalize a referral program, some employers in the high-tech arena have used additional rewards administered through a lottery system. Employees with successful referrals were able to put their names in a hat each quarter for a 2-year lease on a Porsche. The result was that referrals doubled. The providing of a car gave recruiting employees a visible reward that reinforced their ties to the company in much the same manner as health insurance or a 401(k) retirement plan (Frase-Blunt, 2001). Security industry recruiters should look for reward programs that achieve similar objectives.

An additional means of enhancing referrals is through the use of "social network" software. This software enables users to leverage personal relationships for referrals. Monster Networking, ContactSpan, and other sites may aid in recruiting as well as reference checks. The proper mix of technology and professionally trained recruiters may be very effective in certain recruitment markets.

Posters: These placed in strategic locations designed for specific target markets (college students, women, active or reserve duty military, etc.) may bear fruit. Standard paper size announcements that can be produced rapidly hold great potential. Having such a poster that can be quickly downloaded from an employer's Web site may give recruiters a useful tool. If such a form can be e-mailed to college faculty or recruiters in specific geographic locations, the recruitment process can move quite rapidly.

Professional recruiters: These sometimes referred to as "head hunters," may be employed to locate candidates for supervisory positions ranging from line supervisors to senior management. These professional services typically charge a percentage of the starting salary of the candidate to be paid by the hiring organization.

Billboards: These may be an appropriate medium that should not be overlooked. Billboards reach a wider audience and so should be considered as part of a general marketing effort by the organization in addition to their employee recruitment purpose. Advertising space may be donated to public entities as a public service—and potential tax deduction.

Presentations at job fairs, high schools, colleges, and military bases: Traditionally the security industry has not done this to a large extent. It is more common to find public sector police and investigative agencies at job fairs than employers of private sector security personnel. One reason for this is the existence of recruitment officers and teams within public agencies. Having designated recruiters creates a need to send those recruiters out. The cost-effectiveness of this must be weighed, particularly during times when there are no job openings or when the target audience is not large.

Perhaps private employers should consider having designated recruiters. This may help ensure the continuity of the recruitment effort. It could also serve as part of a horizontal promotion scheme: senior officers with certain training credentials would take on additional duties in recruitment. A change in job title or compensation could be part of such a program.

Recruitment stations or offices: These have been widely used by military recruiters who have permanent offices. Temporary offices in shopping centers have also been used. While having a full-time recruiter staff, an office is probably not appropriate for a security employer; it may work for a very large one. It may also be cost-effective via some type of space sharing with another entity. Cooperative recruitment efforts where several employers pool their resources together may also make this a viable strategy.

Academy programs: Running a training academy on a for-profit basis and offering jobs to the top graduates holds some real promise. Contract security agencies in particular may be

able to develop their own staff in a cost-effective manner while simultaneously taking advantage of a built-in recruitment tool.

Intern programs: For college students, these may be used as a recruitment tool. While the main purpose of an internship is to provide an experiential learning opportunity to a student, marketing the organization to the student and the student's social contacts is a side benefit. Word of mouth works extensively as the college also takes on the role of recruiter. Generally internships would be used for reaching out to and getting to know students to fill management positions. They hold great promise in developing future managers. The dearth of management trainee programs within the security industry may be addressed, in part, through the use of internship programs. Intern programs can also be used to recruit entry-level personnel. Offering a former student intern a summer job or a full-time position after graduation is certainly a possibility.

Older interns who are assessing new directions in their careers are being used increasingly within some industries. Baby boomers who have taken early retirement may want to begin a new career. Intern programs allow them to sample the new field. These individuals bring with them knowledge and experience. Such an approach may also be useful within the security industry. Military personnel nearing retirement may be submerged in the culture of a prospective employer.

Employers wishing to start intern programs should be very clear about the objectives they wish to achieve. They must develop goals and procedures. Working with ASIS, the International Foundation for Protection Officers and other organizations can aid in this process.

Extern programs: These consist of having a student "shadow" a job holder during the course of the workday. These may be used in secondary schools that teach Protective Service curricula or colleges that have Criminal Justice programs. As some schools have a requirement for doing a job shadow or ride-a-long, employers may be able to exploit this opportunity quite readily. Schools that don't use externships may be persuaded to adopt them. Prospective students are attracted to programs with such practical components in their curriculums.

Coordinated recruitment: Security employers banding together to pool their recruitment efforts may be a major benefit as pointed out in the following (Leonard and More, 1978) discussion of the advantages of this within the realm of public policing:

1. Creates the possibility of a more widespread recruitment effort,
2. Enables justification for a more sophisticated advertising campaign,
3. Provides the opportunity for recruitment and selection to be handled by professional personnel specialists,
4. Applicants can take a single examination for several different police departments at one time,
5. Potential candidates can be informed of vacancies throughout an entire state,
6. Greater budgetary allocations can be given to the recruitment effort than if a single agency acted alone, and
7. Application procedures would become uniform for all participating agencies.

Policing agencies have in some instances adopted this model. It may be more attractive to them than it would be for security organizations due to the extensive selection costs associated with police officers. The concept does, however, have application to security organizations. Professional associations could potentially play a leading role in cooperative recruitment schemes.

Turnover Costs

Turnover is the number of personnel that remain in a job for 1 year. Positive turnover is few persons leaving the organization. Those who do leave because of retirement, family responsibilities, or promotion within the organization. Negative turnover is a high number of persons leaving a job position. Curtis and McBride (2005) believe that negative turnover occurs when the rate exceeds 10% of the workforce. It is not unheard of in security departments for the rate to exceed 100%, typically within security service firms.

Turnover costs include the funds spent on recruiting, hiring, and training the new employee. While figures given for the cost of turnover vary widely, it is a reasonable estimate that the cost of hiring a new employee is 25% of his or her salary. This may, however, be too conservative a cost estimate in some situations.

Curtis and McBride (2005) maintain that it takes 1 year for a security officer to be trained and to learn the basic job functions. Protection officers must of necessity be intimately familiar with the patrol area as well as the organizational culture. Acquiring such familiarity takes time. With the addition of more sophisticated technology and the potential for expanded duties, more time will be necessary than in the past.

Another concern is the loss of institutional memory. Organizations without people who have seen various approaches to problems taken cannot learn from their history. Experienced employees have an institutional memory, an important asset for any organization that seeks to sustain itself over time.

A cost that is difficult to quantify is the effect that droves of disgruntled former employees may have on the organization. This can take the form of negative advertising —"recruitment in reverse" by ex-security officers who disparage the organization. Such individuals are likely to reveal—and perhaps exaggerate—the organization's "dirty laundry." They will speak of the organization in negative terms, perhaps on Web sites or through e-mails which can reach large numbers of people.

It can also impact civil litigation where a plaintiff alleging negligence can find a number of employees who hold feelings of animosity toward their former employer. Plaintiff's attorneys may then parade a group of them before the court. The volume of evidence may be compelling to the trier of fact.

Internal projections of a negative image may also occur. Security team members are typically in highly visible positions in the organization. High turnover in these key positions can lead to a general feeling of instability toward the organization's security function.

Absenteeism: A Precursor of Turnover?

High levels of absenteeism may be part of a turnover cycle. Employees—particularly those involved in fixed post security functions—may be pressed to work extra hours in order to cover for absent coworkers.

A 2006 survey of 300 HR executives conducted by CCH, Inc. found personal illness (35%), family issues (24%), personal needs (18%), and deserving of more time off (11%) as the major causes of absenteeism (Sopelsa, 2006). A study done in Northeastern Mexico for a contract security firm listed 17 causes for absenteeism. The leading causes of absenteeism according to this survey were a short illness, personal time, holidays, lack of money for commuting, oversleeping, exhaustion because of work, laziness, and attending parties or social events (De Los Santos, 2006).

To control absenteeism, disciplinary action is taken by many employers; 90% of the firms surveyed by CCH did so. While discipline may play a role in controlling absenteeism, there are other measures that may be more effective. In the Mexican study, positive reinforcements were emphasized more than punitive ones. After implementing a series of measures designed to reduce absenteeism, the company's rate dropped from 16 to 10%. Measures included having the officers who missed work fill out a form detailing why they were absent, providing a lecture about absenteeism at orientation, and providing prizes and an annual bonus for security officers who missed work the least. The prizes were things that the officers' entire family could use, such as home appliances, movie tickets, and tickets to amusement parks. In addition to the drop in absenteeism, the reasons for missing work changed to personal time for visiting children's schools, conducting personal business, attending to legal issues, recuperating from short-term illness, and family issues such as caring for sick family members. Frivolous reasons for missing work were no longer major contributors.

De Los Santos (2006) stresses the need to determine precisely what the causes of absenteeism are. In both the De Los Santos and CCH studies, the desire for more time off was a leading cause of unscheduled absenteeism. Sopelsa (2006) notes that Americans have the least

amount of vacation time in the developed world, averaging 13 days per year. The Japanese have 26, Canadians 25, and French 37. Examining vacation and other time off allocations is obviously important.

Keeping employees engaged and making them feel valuable is important. Programs such as compressed workweeks and days, which enable an employee to leave early for a child's school function, are important to employees with children. These programs make employees feel as though they are valued by the employer. Increased productivity and loyalty result from their implementation (Sopelsa, 2006).

Retention Strategies

After recruitment, retaining employees is key to organizational success. Much effort, time, and resources go into new employees. Keeping low attrition is very important to maintaining the day-to-day operations smooth. Employee pay is probably the central issue on why employees move on. Keeping salaries competitive should be a part of retention strategies. Salaries and salary structures should be analyzed by HR personnel (compensation specialists) who assess industry standards, inflation rates, and cost of living.

Realistic job previews are essential. The honesty and integrity of the recruitment effort carries into the retention arena. There is no point in having a "let's get them in the door and started working" perspective as it only leads to decreased morale and subsequent absenteeism and turnover. Realistic job previews can be administered via a video presentation of the workplace or through a personal discussion with a current job holder. Video footage on a Web site or distributed to college faculty to show to their classes can pique the interest of potential applicants while at the same time conveying an accurate depiction of the work environment. This can be done in a short period as video is a fast medium. Discussions with current job holders can provide the personal touch necessary, a touch that is expected by many of today's job seekers. Discussions can include such things as how decisions are made, how much authority employees have, and how people are held accountable (Brandon, 2005).

Make the officers feel unique and special. Distinctive uniforms, job titles, and other symbols of membership in an exclusive group may help enhance "espirit-de-corps." Some proprietary and contract companies provide the uniforms for personnel and even take care of the upkeep. The use of professional titles such as "protection officer" or "security agent" instead of "guard" is one method of doing this. Another is through personality assessments. At the Wackenhut Institute, instructors have used the Myers-Briggs Type Indicator (MBTI) tests to measure officers' personality traits. When the officers see that they are of a personality type that has organizational skills, are good practical problem solvers, and are watchful and loyal, they begin to see themselves as different from the general population. They see that they have something unique that prepares them for a security career (Goodboe, 2002).

Supervisors play a key role in maintaining employee morale and managing retention rates. A long-held management axiom that "line supervisors are the backbone of an organization" appears to be valid. Supervisors are those to whom employees go to with complaints, concerns, and requests. Tulgan and RainmakerThinking, Inc. (2003) found that the routine daily communication between supervisory managers and persons reporting directly to them has greater impact on productivity, quality, morale, and retention than any other single factor.

Organizations must invest in identifying and promoting the best available persons they can as supervisors. The "care and feeding" of supervisors must also be given top priority. Investing in supervisory development programs seems to be a wise decision.

Quality supervision has additional benefits. Top-notch supervisors may be good candidates for promotion to higher level managerial positions. Quality supervision has also been a traditional selling point for contract security firms.

Open door policy: Actively listening to employees is important. This encompasses both work-related and personal issues that confront them. Employment issues brought up by employees may provide clues to larger concerns. Personal issues may not be what the supervisors want to spend their time listening to, but they are important to the employee. Supervisors who believe that they are somehow above being a "shoulder to cry on" are sadly mistaken.

Increased compensation is key to recruitment and retention. Historically low pay was thought to be a problem in recruiting and retaining police personnel. As time went on, defined benefit pension packages and higher salaries came into place. Over time, retention in most public police agencies, at least in North America, is not a major concern. Providing monetary rewards relates Frederick Taylor's Scientific Management theory where workers were inspired to work harder for more money. Tulgan and RainmakerThinking, Inc. (2003) have noted that employers are reducing standard pay and using performance-based pay packages as part of employee compensation.

Benefits are a key part of compensation, especially health insurance. In the United States the affordability of health insurance is a major issue. The amount of money needed to pay for an individual's health insurance is approaching the amount necessary for rent! Organizations that have quality, health, and other benefit programs stand a better chance of retaining employees. Quality programs honestly presented by HR staff in a helpful manner are appreciated.

Training is generally thought to be a key issue in employee retention. Employees see that a professionally delivered training effort reflects the value that the organization places on the officers and the jobs that they do. Officers who have been prepared through preassignment training to handle a situation confronting them are less likely to be overwhelmed by that situation. This may be of particular import when dealing with younger personnel who may expect lots of support from their employers.

One obvious problem is ascertaining its relative import. Organizations that spend time training their employees may also compensate them well. There is evidence, however, from the West Manchester Mall in York, Pennsylvania, which suggests that training by itself without significant wage increases is a key retention technique. The Mall experienced an 85–90% reduction in turnover with only a 7–10% increase in wages. The training process designed by Director Randy Rice consisted of the following steps:

Preassignment Phase

In this phase, preassignment training is given, a large portion of it being the Professional Security Training Network (PSTN) and Basic Security Officer Training Series (BSOTS) which provides a comprehensive introduction to security officers' roles and functions. The series is also designed to help prepare officers for the Certified Protection Officer (CPO) designation.

The Initial 90 Days

Officers are assigned to a Field Training Officer who provides on-the-job instruction, coaching, and mentoring. The staff also completes the PSTN Shopping Center Series to educate the officers concerning shopping mall security. They also complete the FEMA "Emergency Response to Terrorism" course along with regular monthly training on fire extinguishers, OCAT, etc.

The First Year

All officers complete the PSTN Supervisor Series. This is in recognition of the supervisory interface of security officers who are in reality adjunct members of the management team. Such a role is highlighted during emergencies or when the officer is working alone in a facility that is closed.

After One Year

Officers complete the CPO process through taking the CPO Final Challenge Option (Pero, 2003).

Branham (2000) maintains that keeping "Generation X" employees requires them to have some input into the training that they will receive. Letting them know that the employer will provide as much training as possible to develop new skills is important to them. Perhaps this group would be positively influenced by voluntary training, tuition reimbursement, and other programs.

Voluntary training has its roots in policing. Cleveland, Ohio, had a Forum Club in 1910 where police officers would gather on their own time and discuss police issues, sociology, and law (Wadman and Allison, p. 78). Local ASIS chapters or other security organizations could do the same. Law enforcement organizations may use such an approach to develop awareness of emergency management, intelligence, traffic control, and other key areas. Reaching out to "private sector" security personnel can extend the capabilities of the police force. Such an effort may also aid liaison during investigations, emergencies, and public events.

Another approach to voluntary training is to hold weekend or evening classes that provide the officer or agent with a certificate and a meal. Classes in Executive Protection, Counterterrorism, and other "sexy" subjects are likely to generate interest. The title is the "sizzle" and the content the "steak" as the old saying goes:

You need to have the sizzle to sell the steak.

Executive protection would deal largely with manners, deportment, decorum, etc. Counterterrorism could teach search techniques, WMD recognition, etc. Such topics are important for routine operations and safety: proper search of persons entering a secured facility or recognition of dangerous chemicals may be more routine uses of the subject matter.

Tuition reimbursement can be targeted toward those competencies that the employer values the most. It can also aid in organizational development without the enormous cost of employee wages during training. An assessment and ranking of those competencies most desirable would need to be done initially to ensure cost-effectiveness.

Scholarships can take a myriad of forms. Supplying the tuition to a professional growth program for employees who meet certain criteria is one method. Employers can pay for approved training programs for employees who have so much tenure with the organization and have good performance reviews. There are many options to this from Emergency Medical Technician programs to the myriad of offerings given by professional organizations.

Bonuses are often a part of retention systems, particularly in retailing. Annual bonuses or Christmas bonuses give employees something to look forward to and may deter them from leaving the organization. Bonuses can also be used at other junctures, contingent on organizational needs.

Seasonal employers, such as campgrounds, resorts, amusement parks, and retailers, can use bonuses to combat turnover during the busy season. A modest tuition assistance to college students who worked there during the summer may be paid. This could be a small amount per hour that is paid in lump sum at the end of the season. Persons leaving before season's end would not get the bonus. Retaining college students may make good sense as the students will need a job after graduation and may be good candidates for advancement.

Stock options (profit sharing): These should be drilled down as far as possible in the organization. Profit sharing signifies to employees that they are a part of the "team" and that they share in the rewards for successful operations. This is significant in security operations as protection officers are serving as representatives of management. They should be made to feel as though they are a part of management. Additionally they need all the positive strokes they can get. Security works when nothing happens. Unfortunately the only recognition security personnel receive is of a negative nature. Profit sharing—in whatever form it takes—is a positive stroke. Protection professionals need positive strokes!

Retirement plans, such as 401(k) and 403 (b)'s, also signify to the employee that they are part of the organization. There are also options for enrolling employees in Individual Retirement Accounts that employers may wish to explore. Once an employee sees his or her money beginning to grow, they feel more a part of the company that brought them that good fortune.

Promotion possibilities: These possibilities both within and outside of the security function should be considered. Obviously vertical (upward) and horizontal ("promotion in place") options are desirable. The chance to move outside of the security department may also be an option. While the security organization is losing an employee, it is gaining an advocate in another department. Having such an option may help to attract and retain certain candidates whose career aspirations are satisfied by these types of options.

Recognition: Recognition helps to instill pride and confidence in officer ability in both the officer and the organization. There are many ways to do this, from a continuous feeding of the internal newsletter about the achievements of individual officers to "Officer of the Month" programs, annual awards ceremonies, letters of commendation, etc. Officers may be recognized at local ASIS chapters also. Having a "Security Officer of the Year" program is an appropriate activity for ASIS chapters. The event can be publicized in local news media and business publications, giving recognition to the recipient of the award as well as the chapter. It may also be advisable to enable the officers to wear something different on their uniform. A CPO pin is commonly used for this purpose. The astute manager will look to public police and other security organizations for ideas on recognition.

"90-Day celebrations": For newly hired security officers, this early recognition of initial job accomplishments can be key to forming positive images of the employer. Such early rewards may be key to retaining younger employees who yearn for more instant gratification. This is a key point to motivating younger officers who are probably averse to being told they have to "pay their dues" and put in a lengthy tenure in order to advance. Shorter milestones should be integrated within a retention program in order to address this demographic.

Conclusion

Recruitment within the macroenvironment of sufficient numbers of qualified personnel will largely determine the future of the industry. So too will acquiring quality candidates pave the way for success or failure of an individual employer.

The PROTECT acronym may serve as a general guide as to what type of persons are required. This acronym can be used in advertisements directed at potential applicants. It can be tailored to suit the recruiting organization's individual needs.

Prepared to handle problems and crises. Emotionally stable
Reliable. Dependable
Objective and free of prejudice toward particular groups of people. Able to exercise discretion according to the expectations within a professional work environment
Trustworthy. Able to be entrusted with high-value assets and information of a critical nature
Enthusiastic in taking on new challenges; some of which may not be "security" in the strict sense of the term
Career oriented. Seeking to learn and grow within the security industry
Team player. Willing to commit to others, aid them, and sacrifice for them in order to further organizational objectives

Trying to repair a damaged employee–employer relationship is very much like trying to change a tire on a moving car. The best solution for all involved is to make it right from the start. The investment of both care and energy in the selection, hiring, and orientation stages of employment sets the stage for a mutually profitable relationship.

References

W. Atkinson (2005). Hiring older Interns. *HR Magazine* 50(6):139–44.
J. C. Berkshire (2005). Social network recruiting. *HR Magazine* 50(4):95–98.
C. Brandon (2005). Truth in recruitment branding. *HR Magazine* 50(11):89–96.
F. Branham (2000). 10 Ways To Retain Generation X'ers. http://www.amanet.org/books/catalog/0814405975_x.htm. Accessed on October 15, 2006.
G. E. Curtis and R. B. McBride (2005). *Proactive Security Administration*. Wuuper Sadle River, NJ: Pearson Prentice Hall.
G. De Los Santos (2006). Where have all the guards gone? *Security Management* 50(12):38–42.
M. Frase-Blunt (2001). Driving home your awards program. *HR Magazine* 46(2): 109–15.

R. W. Geisel (2004). Interns on the payroll. *HR Magazine* 49(12):89–92.
M. E. Goodboe (2002). How to turn around turnover. *SECURITY MANAGEMENT* ONLINE (http://www.securitymanagement.com/Accessed on January 25, 2007).
S. Grimme and D. Grimme (2007). The secret of retention. (http://www.employee-retention-hq.com/retrieved January 24, 2007).
V. A. Leonard and H. W. More (1978). *Police Organization and Management*. Mineola, NY: Foundation Press.
S. Meisenger (2006). From the president: Workforce retention: A growing concern. *HR Magazine*. http://www.shrm.org/hrmagazine/articles/0406/0406presidentspage.asp
F. Mussano (2006). Personal communication.
J. Pero (2003). Retention through training: A success story. *Access Control & Security Systems*. http//securitysolutions.com/mag/security_retention_training_success/index.html. Accessed on October 15, 2006.
B. Sopelsa (2006). Cough, cough, let's head to the beach: Employers take steps to deal with absenteeism. *York Sunday News*, November 26, 2006, p. H1.
B. Tulgan and RainmakerThinking, Inc. (2003). *Generational Shift: What We Saw at the Workplace Revolution*. Executive Summary RainmakerThinking, Inc. (September 17).
R. Wadman and W. T. Allison (2004). *To Protect and to Serve: A History of Police in America*. Upper Saddle River, NJ: Pearson.

Recruitment and Retention of Security Personnel

Quiz

1. Job shadowing is another term for an externship. ☐ T ☐ F
2. The cost of replacing an employee is generally thought to be equal to 25% of the employee's annual wages. ☐ T ☐ F
3. Newspaper ads can be expected to recruit new applicants as fast as electronic recruitment methods. ☐ T ☐ F
4. Positive turnover is a bad thing for an organization and immediate steps must be taken to control it. ☐ T ☐ F
5. Morale and retention are aided by having quality first-line supervision. Sergeants, shift supervisors, shift leaders, and others are the _____ of an organization.
6. Recruitment and retention ideas should be copied, as appropriate, from police agencies. ☐ T ☐ F
7. Horizontal promotion schemes using Officer First Class, Officer Second Class, and Officer Third Class job titles are also referred to as "promotion in place." ☐ T ☐ F
8. Realistic job previews are a key juncture between recruitment and retention. Without a realistic job preview the retention of personnel is diminished. ☐ T ☐ F
9. Job task analysis is essential for developing a job description on which a recruitment effort can be launched. ☐ T ☐ F
10. Employers should look at the macro level of recruitment in order to create a steady flow of applicants over time. ☐ T ☐ F

This page intentionally left blank

2 Security Personnel Selection

Inge Sebyan Black

If you are a security manager or supervisor, one of your many responsibilities is hiring or overseeing the hiring of security personnel. As you are probably already aware, making the decision to hire someone is one of the most important responsibilities that you will have. People are the most valuable asset your company has, so making the decision to hire someone impacts the success of your company. You will want to remember the phrase, "Hire the right person for the right job." This is really the KEY. Make good decisions based on experience, training, and a solid process and you will be successful. Without careful thought, making the wrong decision can cost your company or even yourself a lawsuit, loss of a client or your job. Hiring the right candidate will also:

- Lower your overhead, increasing your Profit and Loss's
- Lower your turnover
- Increase your retention
- Limit your liability

Let us talk about what goes into selecting the right candidate. Before selecting the right candidate, make certain that you have clearly outlined all the responsibilities in the job description. Once you understand and have spelled out specific job responsibilities, you also need to know the environment, the staff, the management, and the expectations of the key contact. Don't assume anything. Knowing and understanding the role, whether it is an officer, guard, patrol night watch person, or investigator, takes listening so you can hire the right person. By understanding every aspect of the position, you will have the necessary information to make a good decision.

Taking shortcuts to fill a position may be disastrous for your company, so I encourage you to take all the time needed to make the right choice the first time. In today's environment, being cautious about your liability with regards to your security personnel is warranted. Taking shortcuts in the hiring process can cost your company in potential lawsuits. A thorough job description, good interviewing procedures, and a comprehensive background and verification process is essential.

Many companies have a human resource department to write or help write the job description for you. Human resources might also do the recruitment, initial screening/interviewing, backgrounds, and orientation.

Your policies should include that the candidate for security employment have the following:

- Minimum requirements for general employment
- Additional requirements achieved through experience or training
- Additional written, and drug testing
- Capable of meeting the physical demands of the jobs
- Capable of conducting specific duties
- Able to pass a criminal background check
- Does well in the interview process
- Willing to sign the proper disclosures, release forms, and authorizations from candidate

Security Officer Eligibility Requirements

The basics qualifications for most security positions are similar to other industries. The candidate should:

- Be 18 or 21 years of age
- Have a high school diploma or GED
- Have valid drivers' license
- Have the ability to pass a civil, criminal, drug-screening, and employment background check

Some additional standards that are fairly common today are:

- Ability to communicate both written and verbally in a particular language
- Available to work in nights, on weekends, and on holidays
- Some former experience is preferred but not always required

This will make a difference because of the various skills and experience and the possibility of a state license/certificate. No longer are companies looking for a prior military background or law enforcement background. Some of the skills those types of jobs develop are good, others do not always fit the business world as it is today. Being a security officer today, very likely means, applying interpersonal skills to many different types of situations.

- The job requires that a security professional be physically fit.
- Possess decision making abilities
- Be a good fit with the specific environment, whether retail, industrial, bank, or health care, all may require a unique set of skills and character traits.

Being in security today is certainly different than ever before. Companies want their security personnel to know CPR and first aid. They want them to have skills on how to diffuse issues, good customer service skills, and excellent written skills along with being more observant than ever before. The expectation is very high, so it is important to make sure we have qualified people that are appropriately trained. This will add to their success and the retention. Investing in your employees will be the best investment you and your company can make.

No longer does having a background in Law Enforcement or Military automatically guarantee a position in security. Companies now look for security professionals to be part of their team, and not everyone coming from those backgrounds necessarily possess the qualifications. You need to go through the necessary processes to ensure hiring the best fit for that position.

Additional Requirements

Before you write the job description or the requirements, there are several other considerations:

- Does your state have mandated requirements for both the applicant and the testing?
- Have you thoroughly reviewed all of the duties for this position?
- Are there specific state or federal laws that accompany special duties?
- Does the job require carrying a firearm?
- Will they be handling any sensitive and confidential information?
- What, if any, physical requirements are necessary? Will they need to be able to crawl, stand for periods, sit, kneel, etc.?
- Will they be using a vehicle for the position?
- Is vision or a distance ability necessary to perform job?
- Will the person be exposed to any weather conditions?
- Will they need computer skills?
- Will they need to know how to multitask?
- Are the shifts overlapping or will they need to stay on post until relieved?
- If you are a contact security company, the most important question will be, what does your customer want?

The Interview Process

To be successful in hiring the right people, your company needs to have specific policies and procedures that are followed by everyone.

An interview should tell you about the applicant's skills, personality, and work style. You also want to know whether they are suitable for the position they are interviewing for. If you know what traits you need someone to have up front, you will be better prepared to make the right hiring decision.

The interview process should be in several stages, at least two if not three stages. You will most likely be making the final decision on whether this person is a good fit for the position you are considering them for. If you don't have a human resource department, the recommendation is that someone be assigned the responsibility of hiring. That person should be trained and experienced.

You may want to consider administering written tests. These are seen as an added tool when evaluating whether to hire an individual. In the past, testing programs were often used to keep minorities and other persons deemed "disadvantaged" out of jobs. That changed in 1971 when the US Supreme Court handed down a decision (Griggs vs Duke Power) barring "discriminatory" job testing. The courts usually agree that any type of test is acceptable if it can be clearly demonstrated that it is needed to protect the business or its customers from damage or theft, or to protect employees from interference or harm.

Background Check

Since security is synonymous with trust, ensuring a thorough background is done is critical. Conducting a thorough background can involve:

Criminal record check in particular state
Social security check
Motor vehicle record check
Employment verification
Credit check
Fingerprinting for criminal background check (some states require fingerprinting be done on individuals specifically in the security profession)

The Fair Credit Reporting Act (FCRA) governs all aspects of background checks, not just the credit aspect. Under the FCRA, when using consumer reports for employment purposes, employers must:

1. Make a clear and conspicuous written disclosure to the consumer before the report is obtained that a consumer report may be obtained
2. Obtain prior written authorization from the consumer. Authorization to access reports during the term of employment may be obtained at the time of employment
3. Certify to the consumer-reporting agency that the above steps have been followed, that the information will not be used in violation of any federal or state equal opportunity law or regulation, and that, if any adverse action is to be taken based on the consumer report, a copy of the report and a summary of the consumer's rights will be provided to the consumer.

The final process may include drug-screening test, depending on what country you are in. Since 9/11, heightened concern has prompted some legislatures to increase background checks for critical facilities such as nuclear plants.

Conclusion

The key to successful personnel selection means taking the time to hire the right person by performing all the steps in the process.

Security has changed dramatically over the years. We now have our own budgets and offices just like other management personnel. We also are included in management teams.

Because our image has truly changed and become more professional, we must continue to invest in future security personnel. This can only be accomplished by being dedicated to a thorough and well-defined hiring process supported by a comprehensive list of policies and procedures. Once that is in place, compliance with your process is critical.

Security Personnel Selection

Quiz

1. As a security manager, hiring security officers will be one of your most important responsibilities. ☐ T ☐ F
2. Hiring the right person will lower your overhead, increase your Profits, lower your turnover, and increase your retention. ☐ T ☐ F
3. Hiring the right person requires total understanding of the job responsibilities and the environment. ☐ T ☐ F
4. Your employment policies should include specific processes for the hiring and screening of candidates. ☐ T ☐ F
5. Hiring officers for any security role will be the same. ☐ T ☐ F
6. The security role now includes customer service skills, working with other employees in various roles, make decisions, and the ability to multitask. ☐ T ☐ F
7. The expectation of a security person has increased. ☐ T ☐ F
8. Investing in your employees will make your company successful. ☐ T ☐ F
9. The Fair Credit Reporting Act only governs credit reports. ☐ T ☐ F
10. Administering a written test to a job applicant is considered discriminatory. ☐ T ☐ F

3 Supervisory Characteristics and Expectations

Mavis Vet, Charles T. Thibodeau

What is Expected of a Supervisor

Now we come to you the supervisor. Supervision means "overseeing." The National Labor Management Relations Act of 1947 (United States) was more specific and defined a supervisor as "… any individual having authority, in the interest of the employer, to hire, transfer, suspend, lay off, recall, promote, discharge, assign, reward, or discipline other employees, or responsibility to direct them, or to adjust their grievances, or effectively recommend such action, if in connection with the foregoing the exercise of such authority is not of a merely routine or clerical nature, but requires the use of independent judgement."

To properly understand the responsibilities of a supervisor, you have to understand the company structure:

President/directors
Division heads
Middle management
Supervisors
Security officers

The president/director level is where a person or a group of people sets the company objective or the "WHY." In the security industry, this objective is to supply security for a client and make a profit.

The division head level is where the policies are set out. You will find these policies in your company manual, a copy of which you received when you were hired. These policies can also be spelled out in a contract if there is a union. All terms and conditions for employment should be covered along with what the company expects the supervisor to do while in their employ.

The middle management level is the level where procedures are set out for the next two levels to follow. In the day-to-day operations, all terms and conditions of employment must be met following governmental guidelines and union-negotiated clauses while remaining in budget. The middle manager is responsible for ensuring supervisors and security officers to work effectively and develop their full potential for advancement. The more effectively they do their jobs, the less upper management has to be concerned with day-to-day operations.

As a supervisor, you have the hardest job of all the above levels. You have to know and understand all the policies and procedures as set out by the company you work for, what each client expects to be done on their site, and what each of the security officers working for you expects you to do for them.

In a lot of companies, the supervisor will receive little or no training. When you were promoted, you may have been given a set of instructions that covered an explanation of the company, responsibilities of your job, payroll information, and a breakdown concerning the employees under you with regards to the labor laws.

During your career as a security officer, you displayed potential for promotion, including:

1. Job knowledge—you set yourself a standard following the company policies and were consistent in your job performance.
2. Leadership—you have a good reputation with your fellow security officers and clients.
3. Judgment—you have demonstrated good judgment in your decisions when dealing with situations as they arise.
4. Stability—you appear to be level-headed and not on a power trip.

Now as a supervisor, your superiors expect you to take these qualities along with their guidelines and apply them to training, supplying, and directing other security officers.

Characteristics of a Good Supervisor

A very simple definition of supervision would be the accomplishing of work tasks through the efforts of others. At this level of management, supervising versus doing is key. When promoting someone to supervisor the company will look for certain characteristics in the candidates for the job all of which lead to this one attribute: can this person get work done through the efforts of others or must they do it themselves? The following is a short list of characteristics of a good supervisor:

1. Knowledge: know the technical aspect of the job
2. Decisiveness: gather necessary information, review it, make your decision, and put it into effect
3. Communication skills: as a supervisor, you must translate company policy into a plan of action, keep employees informed, assess performance, do appraisals, discipline when necessary, and train or take corrective action. What you say, and how, will affect the morale, attitude, and performance of the people working for you.
4. Establish a work ethic: as a supervisor, you must establish a good work climate, set performance standards with a no-nonsense atmosphere, treat each employee equally while following the established rules, and be accessible to the employees so they know they can discuss problems with you.

Poor Characteristics of a Supervisor

Certainly the candidate trying for a supervisory position who has demonstrated negative characteristics is most likely out of the running and will not get the job. A few of these poor characteristics are as follows.

1. Defensiveness: someone who finds excuses for poor performance and taking all negative comments as attacks on their ability as a supervisor.
2. Lack of emotional stability: quick to anger and frustration when events do not go their way. Does nothing to solve problems.
3. Poor delegation: taking too much on and not being able to finish projects that are started. Not enough time to listen to employee problems. Lacks proper planning to avoid unnecessary problems.
4. Inflexibility: too by-the-book, can cause employees to find ways to circumvent the rules, or openly ignore them in times of need.

The overall result of poor supervision is low morale, poor quality of work, high turnover, and a very unhappy client.

You are to ensure that the security officer working their property has the best guidance to perform the duties according to what the client wants done. It is your responsibility to see that the officers have the proper equipment and the proper training in the equipment's use. If there are any breakdowns of this equipment, you should attend to the repair of it immediately.

Sites should be regularly checked to ensure the safety of the officers working there. Review the officers regularly to maintain the standards set by the company. Follow up on problems or complaints as soon as possible and submit a full report on how to correct it. Above all, professionalism must be maintained in all your dealings.

What Employees Expect from Supervisors

Everyone likes to hear they are doing a good job. Do not be afraid to tell someone they did good work in dealing with a situation no matter how big or small it was. As a supervisor, you must be aware of what all the employees under you are doing. If officers need help, help them. Their problems may seem so small they don't think they should bother getting help, or it may be just a little misunderstanding and easy to correct.

Employers expect clear and concise communication. Proper information flow can clear up a lot of trouble before it starts. Everyone wants to feel they are involved with the company. Rumors can be very damaging to morale. Successful supervisors keep the lines of communication open by giving the employees the information they need to know and keep them up to date on the major events going on in the company.

Employees look to the supervisor as someone they can go to for help. If an employee is not sure of a legality or the proper procedure to handle a situation, they need someone to talk to, and you are that person. If you are not sure of something, let them know you will find the proper answer for them and get it. Always follow up on what you start.

Another aspect of being a supervisor is loyalty to the people working for you. They need to know that in the time of need, you will "go to bat" for them. With this kind of relationship with their supervisor, employees are encouraged to take on more responsibility and develop in their job; they know that if something goes wrong, the supervisor will be supportive and help them through the situation.

One of the most important things that concerns an employee is tactful discipline. No one likes the embarrassment of being reprimanded in public. Everyone wants guidance and feedback on their performance. If you must be harsh with someone, try and offset it with how well the officer performs in general. Always try to give some good with the bad. Remember, these officers reflect on your ability as a good supervisor.

Conclusions

Possibly, the most important cog in the wheel of any successful private security effort is the frontline supervisor. To say the least, he or she certainly must be a multitasker. The supervisor fills the work day with planning decision making, organizing, managing subordinates, and controlling both people and situations. With all these irons in the fire, the supervisor must find a way each day to accomplish individual strategic department and company objectives.

Consider just one of the supervisor's tasks—managing people. Depending on the size of the supervisor's span of control, there could be as many as two dozen subordinates in the supervisor's work group or team. To serve these subordinates, the supervisor must deal with motivation, delegations with follow up and follow through, participation with subordinates in goal setting and decision making, creating and communicating job descriptions, coaching and developing a skilled work force, praising subordinates who do good, and disciplining subordinates who fail to meet minimal department standards.

Does it sound like the supervisors have their hands full? They do! It is our hope that this introduction to supervision exposes some of the challenges that await anyone who might be career minded and wants to take the next step toward management. In addition, we hope that we have not just exposed the tremendous workload carried by a supervisor, but that supervisory activities carry with them real excitement and a sense of a huge accomplishment everyday.

Expectations on the supervisor comes not just from the company they work for, and not just from the client they serve, but from the subordinates they have direct contact with everyday. Meeting everyone's expectations can not only be demanding it can be the exact

exposure the supervisor needs to advance up the management chain to Director of Security. If that is your goal, then security supervision may be your ticket. Good luck and we hope to see you at the top.

Bibliography

Cliff G. Bilya. *The Canadian Manager*. Canada: John Wiley and Sons.
Robert L. Malone and Donald J. Petersen. *The Effective Manager's Desk Book*. Parker Publishing Company.
Robert E. Nolan, Richard T. Young, and Ben C. DiSylvester. *Improving Productivity Through Advanced Office Controls*. Amacom: A Division of American Management Associations.
W. F. Coventry and Irving Burstiner. *Management, A Basic Handbook*. Prentice-Hall, Inc.
David W. Ewing. *The Managerial Mind*. A Free Press Paperback, MacMillan Publishing Company Inc.
William Wachs. *Managerial Situations and How to Handle Them*. Parker Publishing Company Inc.
Kenneth Blanchard and Spencer Johnson. *The One Minute Manager*. Berkley Publishing Group.
Marvin Bower. *The Will to Manage*. McGraw-Hill Book Company.

Personnel: Policies and Procedures

Quiz

1. In the day-to-day operation, all _____ and _____ must be met following _____ guidelines and union-negotiated clauses while remaining in budget.
2. You are to ensure that the security officer works _____ the duties according to what the client wants done.
3. As a supervisor, _____ of what all employees under you are doing.
4. Successful supervisors keep the lines of communication open by giving employees _____ and _____ going on in the company.
5. Understanding on how to _____ you need to _____ for yourself.
6. One of the most important characteristics of a supervisor is leadership. ☐ T ☐ F
7. A security officer's performance reflects on the supervisor. ☐ T ☐ F
8. The company clients' ideas are important in how to train a security officer at their site. ☐ T ☐ F
9. During the performance of your duties, flexibility is not a major concern. ☐ T ☐ F
10. As a supervisor, it is important to understand the company structure. ☐ T ☐ F

4

Evaluation of Uniformed Protection Officers

Ronald R. Minion

Introduction

The line security officer plays a vital role in the success of any security organization. The level of motivation also creates an immediate impression regarding the organization he/she is responsible to protect. First impressions are lasting!

During my 33 years tenure in the contract security business, I have worked with high/medium/low performers. A high performer does not necessarily make the best officer. Who gets the job done the best? A long-term solid performer, a protection officer who has been properly screened, trained, uniformed, and properly prepared for the job of protecting life and organizational assets.

Once the officer is on the job, far too often security managers take the approach; "we're done, out of sight/out of mind." Wrong; this is the time when all officers need guidance/support in order to get the job done effectively. Good supervision/coaching leads to positive performance, performance that builds profits (contract or proprietary).

There is no magic to motivate the uniformed security officer. But, for too long, guard force managers have not paid enough attention to the officer's individual professional employment needs. The job can't get done without expending human and financial company resources for officer's support/leadership/professional development.

These two resources are indeed precious; hence, you must have a program, a plan that will work. Once you commit organizational resources to employee motivation, you had better known what you are doing, how the resources will be managed.

I have owned/operated two successful commercial contract security companies. Both were managed on the premises that the "bottom line" profit resulted directly from the level of motivation of the line security officers. How company resources are expended to enhance motivation/productivity within the security force is a very important exercise in human resource management! The following step-by-step program may seem like a departure from the traditional way protection officers are managed.

Officer Evaluation

Before we discuss rewards/perks/bonuses, we must have an accurate record of how well our officers are doing. This can't be a "hit-miss" opinion expressed by a supervisor. We have to score/grade each officer. A report card must be designed/generated. Grade the officers and then grade the site/account. This is the beginning of the "team approach" to guard management. The following questions must be addressed:

How do we evaluate the officers?

- What are the criteria?
- Who conducts inspections/evaluations?

- How do we verify results?
- How do we link officer performance to team performance?
- How do we "feed-back" results to officer(s)/team(s)?
- What are the rewards for good performers?
- What are the sanctions for bad performers?

Step #1

We must determine what job related officers' accomplishments/performance are most important in the evaluation process. The 10 most important factors to be assessed are as follows.

Dress/Deportment

How well the officer turns out and conducts him/herself on the job will be a determining factor in the level of performance. How often have you seen a sloppy officer perform well? Have you seen a crisp/sharply turned out officer perform below security management's expectations? The officers must have the tools to work with—a good uniform management program is essential.

Qualifications

There are numerous training/education opportunities available for protection officers. There are official certifications that accredit the officer's achievements/skills. The most important training programs directly linked to officer performance are First Aid, CPR, Non-Violent Crisis Intervention, Occupation Health & Safety, Certified Protection Officer (CPO), Protective Security Courses at private/government institutes, and professional college security programs leading to an associate or bachelor's degree.

Reports/Notes

The officer who is capable of effectively taking notes during his/her tour of duty and able to translate the information to a useful report is vital to a successful security department. Electronic incident tracking often replaces the manual process; hence, officers must be familiar with how to use computers. Good security depends on officer's contributions to record keeping and statistics.

Site Operating Procedures

All levels of the security unit should participate in the development and maintenance of effective Standard Operating Procedures (SOP). Once these indispensable orders are complete, they must be continually updated. Good officers work hard at keeping security procedures current. Officer's knowledge and understanding of the application of site/post orders significantly enhances security.

Knowledge of Site and Facility Orientation

Prior to permanent assignment to any post/site, the officer must be familiar with the physical layout of the property/facility to be protected. Site plans, supervised tours, duty checklist, SOP, and a written quiz at the completion of on-the-job orientation are all helpful in gaining a clear understanding of the physical plant.

Attitude

An officer with a positive attitude toward his/her employer, duties, responsibilities, and the site, which must be protected, is essential for good security. Bad attitudes equate to bad security. An officer who has assumed a position in security as a "stop-gap" measure will seldom possess the right attitude. Good attitudes are developed through joint goal setting. Officers who have a say in how site security is managed generally have the best attitudes.

Public Relations

The protection officer is a public relations envoy for the organization he/she protects. The officer who has paid attention to the need for appropriate dress and deportment has taken the first step in the creation of a positive first impression with visitors, employees, customers, and corporate executives. The officer must understand how to be portrayed as the person in charge. An individual who exhibits a pleasant/upbeat image is vital to a successful Public Relations Program.

Reliability

The ideal officer will come to work early to make sure he/she is fully conversant with the events of the previous shift. Once management recognizes an officer as reliable, he/she will be given more responsibility, advancing a professional career in security. This officer knows his/her work, understands SOP, and works harmoniously with other officers on the security team.

Housekeeping and Image Enhancement

A sloppy officer, a sloppy security office, sloppy records, sloppy notes, sloppy reports all lead to poor performance and poor security. In the overall pursuit of image enhancement, protection officers must work at looking sharp at all times. They must keep the security area tidy and maintain orderly records and reports. Good housekeeping equates to good security.

Permanency

Turnover is an ugly word in the private security community. New faces create most deficiencies in the life safety/asset protection program. The qualified officer who dresses immaculately, produces quality reports, understands SOP, has the right attitude, exhibits public relations, is reliable, and keeps a tidy work station will stay longer, feel good about the job, and will be a credit to his/her employer and the security profession.

Step #2

Evaluation Format

All employees, regardless of their occupation, need feedback. "How am I doing?" "How does my work compare with my coworker's?" "How can I improve?" Protection officers are no exception. If they are left in the dark and can only guess as to how well they are getting their work done, they will soon become demoralized, negatively impacting performance.

The following officer appraisal forms have been developed to accurately assess performance. These reports are based on the 10 most important factors necessary for the attainment of officer's success in the security workplace.

Ten success factors each graded 1 to 10. (1—unsatisfactory 10—outstanding)

Inspection Report Officer Evaluation Form

Date: _____ Time: _____ Site: _____

Inspector: _____ Officer: _____

Evaluation Results

Please check mark in applicable box. (See reverse for guidelines.)

	1	2	3	4	5	6	7	8	9	10
Dress/Uniform										
Qualifications										
Quality of reports/notes										
Knowledge of orders										
Knowledge of site										
Attitude										
Public relations										
Reliability										
Housekeeping										
Permanency at site										

Add up all values of the check marks and enter the total: (Maximum possible □ 100 points)

Total: _____

Comments: _____

Officer: _____

(Signature) Date: _____

□ □ □

The form below illustrates grading criteria, showing what the inspection coordinator looks for to establish scores.

□ □ □

Inspector notes: Place a check mark in the appropriate value box for each category, e.g., if an officer has four out of five of the requirements for dress/uniform, place a check mark in the box under 8 against dress/uniform. One point may be awarded in situations where the officer does not fully meet the required standard, e.g., shirt is clean but not pressed, not fully conversant with content of orders, etc.

Dress/Uniform	2 points each for: Pants/skirt clean and pressed Footwear correct style and clean/polished T-Shirt or tie, clean and of correct form	Shirt/blouse/jacket clean and pressed

	Hair—Men short, clean and clean shaven Hair—Women short, up and off the collar, clean	
Qualifications	2 points each for: NVCIT OH&S CPO Others	First aid/CPR
Quality of reports/ Notes	2 points each for: Notebook—correctly used Report—neat and tidy Report—properly completed Report—easy to understand	Notebook—possession
Site operation procedures	2 points each for: What is covered in orders Interpretation of orders Application of orders Basic knowledge of orders	Location of orders
Knowledge of site	2 points each for: Location of exits/entrances incl. fire exits Locations of high security areas Location of alarm panels General layout of building, area, and lighting	Location of fire suppression equipment
Attitude	Look for: Initiative Personality type Enthusiasm	Problem solving skills
Public relations	Look for: Impartiality Consistency of approach Compliance to procedure	Courtesy, restraint, and interest
Reliability	Look for: Adherence to work schedule Willingness to work extra shifts Does the officer do the required job?	Punctuality
Housekeeping	Look for: Professional appearance of work area, etc.	Accessibility of orders, stationary, forms, etc.
Permanency at Site	2 points for each month on site, 10 points for 5 months or more	
Rating structure	2: Unsatisfactory 4: Requires improvement 6: Satisfactory—room for improvement 8: Satisfactorwy—meets requirements 10: Outstanding	

(Continued)

Interpretation	20—40 Officer is unsatisfactory for site 40—70 Officer requires improvement 70–90 Officer is satisfactory 90+ Officer exceeds requirements

Step #3

Evaluation Process

The completed evaluations are invaluable documents that can be used extensively as a protection officer management tool. To effectively evaluate all officers on a particular site, a senior member of the force must be appointed to coordinate the project (inspection coordinator).

The inspection coordinator must work closely with the site supervisor, communicating proactively. The exercise must not be deemed as a "witch hunt," rather a positive program designed to recognize good work by all officers.

Once all of the evaluations have been completed, they must remain confidential and be delivered to a senior member of security management (Figure 4.1).

Step #4

Officer/Team Assessments

Based on the above described collection of data, security management will be in possession of very valuable information that should not be left to gather dust. This data that has been assessed by the inspection coordinator must be discussed with the site supervisor (see Figure 4.1).

Each officer must be given the opportunity to discuss his/her appraisals. It must be an exercise designed to enhance motivation/performance. It is time to set goals, rather than chastise. Each officer must be told of any shortcomings brought to light in the performance audit. Each officer must be told of the timing of the next evaluation and instructed on how to improve performance as required. By calculating each officer's rating, it is easy to determine a team score. Simply take the average of each officer's score, including the supervisor(s). Now you have officer/team grades. So what do you do with this information? The results have been discussed in private with each officer, you must discuss the ratings with the team.

And the client, not only the commercial customer but corporate management, will be impressed with company security professionals who have worked hard to develop a productive security organization that is staffed with officers whose performance is measured, a process that provides guidelines designed to eliminate bad performance among the protection service group.

We now have a level playing field; each officer knows the rules. All team members must be informed as to when and what to expect from the next scheduled inspection, which should be conducted within 6 months.

Step #5

Goal Setting/Motivation

It is time to set realistic goals. If the overall average was 70%, set a new target of 75%. This gives everyone on the team something positive to strive for. It will be amazing to see how (without any help from management) the team will establish a norm for good performance. Now, team members will discreetly sanction poor performers and sometimes not so discreetly. Everyone wants to play on a winning team.

Ideally, there should be more than one team. If the team consists of a small proprietary security force, make each shift a separate team. If it is a large in-house group, identify each site as a team. If it is a contract company, the number of teams are unlimited.

Team standing will become very important to team members, but only with management impetus. The entire evaluation program has to be managed. Communicating information is

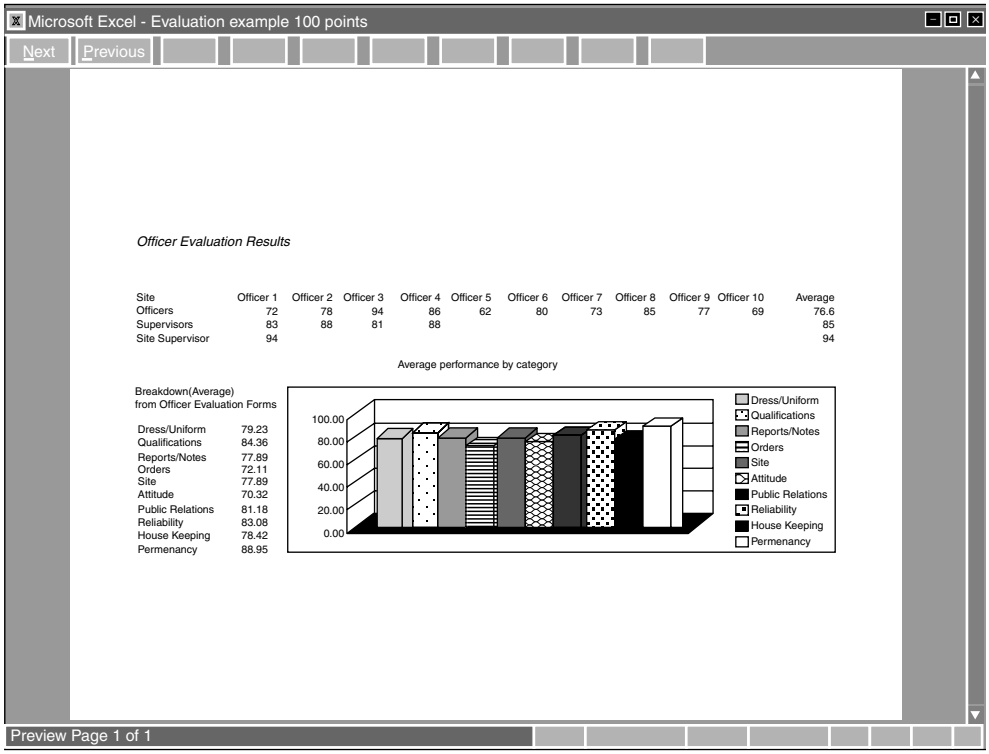


FIGURE 4.1 Results computed to depict officer and team performance ratings.

vital to the overall success of the program. By placing a lot of emphasis on the results of the evaluations, management can significantly improve overall officer performance.

If management, supervisor(s), officers, and teams think the results are inaccurate, how can the rating be validated? If the accuracy of the grades is in doubt, a private security consultant, a member of the HR, or other department within the organization can be recruited to do spot audits to confirm the correctness of the data.

How do you sanction poor performers? Certainly a confidential corrective interview is in order. If the deficiencies are serious, issue a written warning. But most important, allow an opportunity to improve. Turn a negative to a positive by skillfully communicating with the low-scoring officer. Individual coaching and encouragement will go a long way to improve future evaluations.

How do you reward officers? A letter of recognition, a certificate, a plaque, a bonus, gift certificate, a promotion, a lapel pin, medal of merit, dinner with the boss, a promotion.

How do you reward teams? Publish the standings, tell other departments/divisions in the organization, a write-up in the company newsletter, monetary reward to be divided by team members, team jackets, crests, individual/group certificates/plaques, pizza party.

The perks/rewards from the initial audit should be minimal. Wait for the results of further audits. Rewards should only come after a year. For example, an achiever who continually scores more than 80% ratings may be allowed to use an internal security designation, such as medal of merit, after his name. It is prestigious, and officers like recognition.

Most important, however, our goal is to improve performance through heightened motivation within the security organization. The perks/rewards are secondary to improved on-the-job officer performance.

How to measure officer performance has always been a puzzle; you now have the right yardstick!!

Motivation and Evaluation

Quiz

1. The _____ security officer plays a vital role in the success of any security organization.
2. The job of motivating the officer can't be done without expending _____ and _____ company resources.
3. Electronic incident _____ often replaces the manual process.
4. All professional employees, regardless of their occupation, need _____ regarding performance.
5. Our goal is to improve _____ through heightened motivation.
6. Security officer motivation has little to do with organization "bottom-line" profit. ☐ T ☐ F
7. How the officer is turned out for duty has little to do with performance. ☐ T ☐ F
8. The security officer is responsible for preparing Site Operating Procedures. ☐ T ☐ F
9. Good housekeeping is a vital part of the overall security operation. ☐ T ☐ F
10. Perks/rewards as a result of the initial audit should be minimal. ☐ T ☐ F

5 Employee Motivation Theory and Application

Eric Webb

A motivated and emotionally engaged workforce is critical in any employment environment; and even more so in the area of public safety and asset protection. Creating an environment where staff feels appreciated, valued, and challenged develops a sense of pride and belonging in employees. Employees that appreciate and value their employer and associated job responsibilities are less likely to leave the organization, miss work, or expose the employer to liability and risk.

While the benefits of a motivated work force are obvious to the novice manager, creating an atmosphere that fosters employee participation and motivation is difficult for even the most experienced supervisor or leader.

Unfortunately, there is no formula for fostering a positive engaging work environment. Each individual employee is unique and presents different characteristics, history, and personality traits that may or may not respond to motivational techniques. The key to creating an environment that develops loyalty, creativity, and appreciation in employees lies within understanding the basic psychology of motivation and administering techniques diverse enough to meet the needs of heterogeneous employees.

As each organization is different, so are the keys to fostering motivation in those organizations. In this chapter, we will review basic concepts of motivational theory. These theories, coupled with creative thinking, can provide management of the tools to create unique, effective, and responsive programs and policies that keep employees interested and engaged.

Theories of Behavioral Motivation

Maslow's Hierarchy of Needs

Through extensive research and analysis, social psychologist Thomas Maslow developed his well-respected theory of human motivation and responsive behavior (Huffmire, 117). Maslow's hierarchy of needs attempts to explain human psychological and social development through a series of progressive needs and desires that once fulfilled motivate the individual to develop the desire to pursue then satisfy the next subsequent and escalating need. To understand Maslow, one must meet the first need in its entirety before engaging the next need (Figure 5.1).

Maslow's theory entails five fundamental human needs:

Level 1: Physiological needs: food, shelter, clothing
Level 2: Safety needs: self-preservation
Level 3: Social needs: a sense of belonging and acceptance
Level 4: Esteem needs: self-esteem and recognition from external sources
Level 5: Self-actualization: to fully realize your full potential

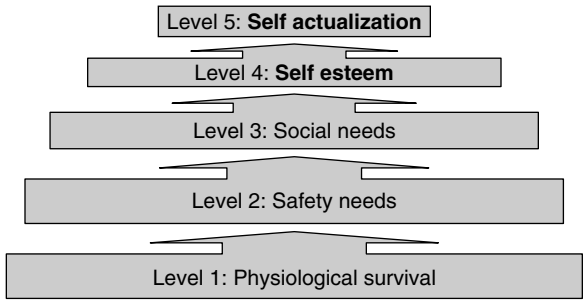


FIGURE 5.1 Maslow's hierarchy of needs.

There are three fundamental concepts Maslow promulgated in understanding his hierarchy: (1) behavior is affected by unmet needs; (2) individuals meet their most basic needs first and then escalate; and (3) fundamental needs take precedent over advanced needs (Muchinsky, 376).

Maslow's levels of motivation translate well into the work environment. Each level can be related to an employee from their initial hiring through promotion, training, and leadership. Understanding where an employee is within the organization with reference to Maslow may help management and supervisors determine the appropriate motivation and rewards for that individual.

For example, according to Maslow the most basic fundamental needs of an individual (physiological and self-preservation) will motivate the applicant to seek employment. Employment offers the ability to provide food and shelter (Maslow's Level 1) and a means to maintain those achievements (Maslow's Level 2). A new hire can be classified within these paradigms. They have been motivated to seek employment with your agency in order to meet fundamental needs. The new employee is initially focused on learning the job in order to maintain employment that fulfills his need for self-preservation.

Remember, Maslow argues that individuals accelerate through the hierarchy of needs (Huffmire, 117). As one need is met, the next level of desire becomes essential. After an employee has met their basic needs and learned the skill set required to maintain employment (Levels 1 and 2), Maslow's hierarchy would suggest the employee to begin to seek acceptance from coworkers and staff. Basically, once an employee understands how to do the job, they will seek to create social bonds with those they are sharing the work environment. An employee at this stage may be receptive to programs or trainings that foster a sense of teamwork or allow them to work with individuals they normally wouldn't have an opportunity to meet. An employee at this stage may be receptive to shift work or overtime simply to expand opportunities to meet and relate to other members of the organization. Clearly, a new employee would not be an appropriate candidate for extensive rotation, overtime, or additional responsibilities as they are still engaged in a lower level of motivation. The new employee is focused on how to do the job in order to retain the job.

Once an employee has internalized the skill set required to be successful and has exercised opportunities provided by management to network within the organization, the next step in Maslow's theory is likely to develop. Level 4 of the hierarchy of needs seeks to meet self-esteem needs. At this point, the employee will be comfortable enough within the context of the organization to desire to contribute to the overall welfare or betterment of the operation. This may be the most difficult stage of effective management, but it also offers the most opportunity to motivate, develop, and retain effective employees. An employee desiring to fulfill esteem needs will want to feel appreciated and needed within the corporation. This likely will manifest itself in employee's suggestions to management, recommendations for improvements or changes in operating procedures, or even employees volunteering time or experience to contribute toward new ideas or procedures. A manager that listens to employee's suggestions and takes them into consideration is more likely to foster a sense of loyalty than one who immediately rebukes such

ideas. Even employee input that cannot be implemented offers management an opportunity to foster motivation. By communicating the reasons why a process cannot be adopted, coupled with appreciation for the employee effort and input, management can instill the feeling of participation among the staff, thereby fulfilling the esteem needs of employees.

The final component of Maslow's need-based hierarchy entails self–actualization, in other words, a need to fully meet your personal potential. Not every individual or every employee ever reaches this final step. Employees that do not feel valued by the organization or are constantly changing jobs and therefore have not met their self-esteem or more fundamental needs will not seek to fully address their potential as an employee. However, individuals within an organization that do feel valued and secure in their employment will look for ways to make their experience even more fulfilling. At this point, management should have in place programs for tenured staff that affords opportunities to achieve higher professional and personal goals. These individuals will seek to continue their education, obtain professional certifications, or even cross train within the organization to learn new skill sets. While this is the ideal scenario, an employee seeking to become as well rounded and valuable as possible will only do so after he has been properly trained, socialized, and recognized within the company.

While Maslow's theory certainly does not address every problem associated with employee motivation, it can be used as a guide to assist managers in determining where an employee is within their work experience and subsequent appropriate motivators to be used to foster that employee development and motivation.

Herzberg's Two-Factor Theory

In contrast to Maslow, Frederick Herzberg theorized that motivation (specifically in the workplace) is influenced by nonexclusive factors of job satisfaction and dissatisfaction (Riggio, 195). Herzberg surveyed workers to determine what they appreciated about their jobs as well as what frustrated them about their employment. Herberg's finding resulted in his Two-Factor Theory.

Herzberg suggests that when certain factors are present they can provide motivation for employees. Herzberg simply and directly calls these motivating factors "motivators." Conversely, when other factors are absent, workers become frustrated and unsatisfied. Herzberg refers to these factors as hygienes (Riggio, 195).

The Two-Factor Theory argues that successful managers must reduce job dissatisfaction by providing employees with hygiene factors (Riggio, 195). These factors tend to relate to the environment in which one works and the context of that work. By providing safe-working conditions, a reasonable salary, and benefits, employers meet the hygiene needs of their employees.

However, to truly engage and motivate employees requires that motivators must be implemented to encourage employee loyalty and growth (Riggio, 195). Motivators include factors related to employee self-esteem and actualization. Common motivators may include responsibility, advancement, and recognition (Riggio, 195).

In effect, Herzberg's theory may be readily combined with the ideas presented by Maslow. Where Maslow would argue fundamental needs must at first be met, Herzberg would see hygiene factors that require satisfaction. Maslow's subsequent pursuit of self-esteem and self-actualization is then reflected in Herzberg's motivation factors.

Many theorists actually combine the theories of Herzberg and Maslow into a single hierarchy of needs; but for the purposes of this text, it is important to understand the unique concepts Herzberg presents to add to our understanding of employee motivation.

Reinforcement Theory

On a more fundamental level, Reinforcement Theory seeks to explain motivation by examining consequences (Riggio, 189). Knowing the result of certain behavior can affect the motivation of an individual to repeat the same behavior. Realizing positive benefits through exceptional performance motivates employees to continue to strive to excel. Reinforcing positive behavior

with rewards motivates employees to continue that behavior. Subsequently, reinforcing negative behavior with sanctions deters employees from repeating certain actions.

In the security environment, it is all too easy to reinforce negative behavior through reprimands and sanctions. While it is certainly an occasional necessity, it often becomes the focus of supervisors in a paramilitary organization. Successful managers are those that take the time and initiative to communicate positive reinforcement to their staff. While rewards, benefits, and time off are excellent positive motivators, they may not always be practical or financially possible. Simply recognizing performance and expressing gratitude for that performance may be enough to foster a proactive environment where employees feel valued.

It is important to think creatively when implementing positive reinforcement. Employee of the Year (or month) programs can provide a cost-effective and easy opportunity to recognize performance. Progressive security employers do this in many cases. Couple the employee award with a premium parking space or company token of appreciation, and you now have a cost-effective positive employee motivation program in place that requires minimal administration.

Equity Theory

The Equity Theory introduced by J. S. Adams in 1965 postulates that individuals make generalized calculations about their relative contributions and rewards extrapolated from their employment (Muchinsky, 378). An employee will evaluate the time, effort, and skill they contribute to an organization and compare that with the benefits of the aforementioned employment: pay, health care, hours, etc. What this theory basically states is that employees will determine for themselves if their effort is being justly compensated. Adams' Equity Theory proves invaluable when it is used as a tool to analyze effort and rewards between employees.

Equity Theory argues that when employees put in relatively similar inputs but receive dissimilar benefits, work place stress and anxiety will occur (Muchinsky, 378). The employee receiving less benefit is more likely to be absent and disinterested in his work. If the employee perceives that his effort is being less appreciated than similar efforts from other employees, the disappointed employee will not be motivated to contribute to the organization (beyond the minimal requirement to maintain employment).

Using Equity theory does not mean all employees must receive the same pay or benefits package. The theory recognizes that employees are making calculations based on perceived efforts and inputs in the work environment. An employee can recognize and appreciate another individual in the organization earning a higher wage if that person's experience, skill, and knowledge are readily apparent. The problem in this theory develops when employees of similar abilities begin to perceive unequal benefits derived from congruent employment.

While there are additional pieces of Equity Theory, it is imperative that security management professionals recognize that employees make these "work effort" calculations constantly. It is impossible to properly motivate an organization if members of the team do not feel they can get a fair shot at participating and earning benefits from the employer.

Practical Tools in Fostering Motivation

While theory is helpful in explaining employee needs and behaviors, managers need to perform and supervise staff in the real world. Effectively managing and serving the organization is infinitely easier with a highly motivated and responsive staff. What tools can be easily exercised to foster such cooperation?

Leadership: Possibly the single most important factor in motivating employees is in the behavior and professional demeanor of senior staff and executives. Effective leadership is not necessarily the result of a magnetic personality; many quiet unassuming individuals have proven to be exceptional leaders (Huffmire, 24). The diminutive James Madison and boisterous Theodore Roosevelt prove that diverse personalities can be successful in motivating and

managing people and organizations. To provide effective leadership for an organization, one must present clear goals, clarify responsibilities, and nurture increased authority in subordinates as their skills develop and grow (Huffmire, 24).

Participation: Providing employees input into the decisions that affect their environment is one of the most effective tools in fostering motivation. The more people feel they were involved in a decision, the more personal ownership they will have in their work (Allen, 176).

Training: Normally, a discussion of training needs for security staff focuses on new hire orientations, use of force, sexual harassment, and legal issues; however, training can be a powerful motivator for employees. Beyond the rudimentary training provided to all employees, managers can reward employees' interest and efforts through formalized training programs. When management recognizes an innate skill or trait an employee possesses, offering a formalized training program serves not only as a positive reinforcement for the employee but also a possible financial benefit for the organization. For example, having an employee that helps around the office with computer problems may provide an excellent opportunity for management to encourage formal computer network training at a local trade school. The employee obtains valuable experience and possible certification and management now has a multiskilled team member capable of saving the organization's time and money.

Rewards: Possibly the most difficult thing a manager can do is implement a good employee reward program. Very few security budgets contain line items for employee rewards, nor is there ample petty cash available to meet this need. Fortunately, rewards can be implemented fairly cheaply if done with a little bit of creativity. Rather than large cash awards, simply providing monthly recognition in the form of an employee of the month reward can foster a sense of pride in an organization. Rewards can range from something as small as a certificate of appreciation or a desirable parking spot to additional time off or restaurant vouchers. Regardless of what type of reward management chooses to provide, it must be done by leaders who are sincere and can effectively communicate with employees. Even the smallest reward when coupled with sincere appreciation can provide the valuable positive reinforcement that addresses an employees desire to feel valued within an organization.

Summary

Various theories of human behavior and motivation seek to explain why individuals react to specific situations. In the workplace, it is critical to understand behaviors and needs that motivate employees. The new hire and the old veteran may come to work in the same environment and perform essentially the same duties, but they may have dramatically different psychological motivations in performing that work.

An effective manager should understand the various theories of human motivation, and use those concepts to address the needs of individuals throughout the organizations appropriately. Understanding what someone needs to reinforce or motivate positive behavior is critical in fostering high-achieving, motivated employees.

While understanding such concepts are important, implementing appropriate solutions in the real world can be challenging. Managers can use a combination of rewards, training, employee input, and leadership to motivate staff. Assessing the various programs in use by both security and nonsecurity organizations is a good place to start.

References

A. Louis (1973). *Professional Management: New Concepts and Proven Practices*. Berkshire, England: MacGraw-Hill.

D. Huffmire and J. Holmes (2006). *Handbook of Effective Management: How to Manage or Supervise Strategically*. Westport, CT: Praeger Publishers.

M. Paul (2003). *Psychology Applied to Work*. Pacific Grove, CA: Thomson Wadsworth.

R. Riggio (2000). *Introduction to Industrial/Organizational Psychology*. Upper Saddle River, NJ: Prentice Hall.

Employee Motivation Theory and Application

Quiz

1. Maslow's hierarchy of needs contains three critical steps. ☐ T ☐ F
2. Leadership is not an important factor in employee motivation ☐ T ☐ F
3. Equity Theory is concerned with a "fair" relationship between effort and reward. ☐ T ☐ F
4. _____ authored the Two-Factor Theory.
5. According to Maslow, the most fundamental need for human beings is self-esteem. ☐ T ☐ F
6. Training may be used as a reward or motivator in some organizations. ☐ T ☐ F
7. Most agencies do not have funds budgeted for employee motivational programs and therefore managers must be creative in creating effective opportunities to motivate staff. ☐ T ☐ F
8. Name the two types of reinforcement under Reinforcement Theory:
   1.
   2.
9. According to Herzberg, workers become frustrated when hygiene factors are absent. ☐ T ☐ F
10. Employee participation in decision making and policy development can foster a sense of ownership and motivations. ☐ T ☐ F

6

Employee Discipline: Policy and Practice

Brion P. Gilbride, Michael J. Apgar, and Todd Staub

One of the most unpopular duties of a security manager is to discipline a subordinate employee/officer. The reason for its unpopularity rests in the difficulties involved in initiating the disciplinary process, regardless of the organization in which this occurs. Here, we will define *discipline*, explain when it should be used, and most importantly *how* it should be used.

Defining Discipline

Discipline is, basically, an action taken by a supervisor to correct the behavior(s) of a subordinate employee, generally within that supervisor's department. A good manager "must be prepared to discipline when the need arises."[1] It is helpful to remember that many problems are not deliberate actions on the part of an ungrateful employee, but honest mistakes caused by inexperience, lack of education, or improper socialization. An organization's rules and policies are written to address "routine, day-to-day events."[2] Discipline is generally not looked on favorably by both supervisors and subordinates, so the least severe action taken to correct a problem will usually be the most effective.[3]

If these two ideas are combined, most disciplinary problems will not result from catastrophe, but from normal operations. For example, Stephen Robbins mentions in his book, *Personnel: The Management of Human Resources*, that "The most serious discipline problems facing managers undoubtedly involve attendance."[4] Next to that are "on the job" behaviors, such as "insubordination, horseplay, righting, gambling, failure to use safety devices, carelessness, and … abuse of alcohol and drugs."[5]

> *Discipline is usually prompted when a mistake is made, often in the form of a wrong decision.*[6]

---

1 H. Burstein (1996). *Security—A Management Perspective*. Englewood Cliffs, NJ: Prentice Hall, p. 72.

2 A. R. Stone and S. M. DeLuca (1985). *Police Administration, An Introduction*. NY: John Wiley & Sons, p. 344.

3 G. O. Stahl (1971). *Public Personnel Administration*. NY: Harper & Row Publishers, p. 310.

4 S. P. Robbins (1982). *Personnel: The Management of Human Resources*. Englewood Cliffs, NJ: Prentice Hall, p. 394.

5 Robbins, p. 393.

6 Burstein, p. 72.

Employees

Employees are all unique to themselves, and it is important for supervisors to understand the fact that each person must be dealt with differently. Most employees, however, fit into one of five different groups: political, aesthetic, social, economic, and theoretical. Each of these groups may contain either professional employees or problem employees depending on how each specific person chooses to deal with his/her own personality (Pollock, 1999).[7]

Personality Types of Employees

There are five different personality types of employees that come into the work force. They are political, aesthetic, social, economical, and theoretical. It is very important and essential for supervisors to understand the different types of employees because every employee will fall into one of these types of employees, and understanding the types of employees will allow a supervisor to give assignments in the manner that fits that type of employee; therefore, the supervisor can actually reduce the need for discipline because assignments are made specifically for each type of employee. The five personality types are as follows:

1. Political: This type of employee can be very intimidating to both other employees and their supervisors. Their personality is controlled by aggression, demands, authority, and control, which could either lead to a successful professional employee or to a very difficult employee. Being given some authority and control can motivate political employees. Supervisors should give these employees the results that are expected and the day it should be completed by; however, let the employees decide how to get to the expected results.[8]
2. Aesthetic: These are the employees who base their success on their creativity and usually need a lot of room to use their imagination throughout their work. Freedom to work as they please is a necessity for this type of employee. Aesthetic employees take more time to complete assignments than most employees, so it is essential that they are given an adequate amount of time to complete an assignment.[9]
3. Social: These employees work well with others and are generally productive. However, if they do not have enough to do, they may disturb other employees from completing their jobs. These employees are often the ones who speak without thinking and need time limits in order to complete tasks. Make sure that these employees have plenty of work to do and that they are given deadlines for assignments.[10]
4. Economic: These are the employees who are very detailed, good planners, and usually do things "by the book." These employees are analytical by nature and are motivated by information. Also, these employees tend to spend a lot of time completing simple tasks. Do not let these employees spend a lot of time on simple assignments; instead, explain to these employees why assignments need to be completed by deadlines.[11]
5. Theoretical: These employees are "highly technically skilled people." Many times, these employees may know more about a specific job than even their supervisor. This group of employees will often try to use other employee's ideas as their own, not knowing that the idea is not original. Make sure these employees are given deadlines for assignments and allow them to think out ways to complete tasks, thus giving them a sense that the ideas they came up with are their own.[12]

---

[7] I. E. Pollock (1999). Dealing with difficult employees. In *Security Supervision: Theory and Practice of Asset Protection*. Woburn, MA: Butterworth-Heinemamn, p. 72–75.

[8] Pollock, p. 72–75.

[9] Pollock, p. 72–75.

[10] Pollock, p. 72–75.

[11] Pollock, p. 72–75.

[12] Pollock, p. 72–75.

Protection officers will fall into one of these five employee personality types; however, supervisors should understand that out of these five personality types come the professional employee and the problem employee.

The Professional Employee

According to Dale June, a professional is defined as "one worthy of the high standards of a profession" and as "having much experience and great skill in a specified role."[13] These people understand the specifics and details of their job. Every profession has organizations that members belong to and a very specific professional code of ethics that employees are to follow (Hertig, 1998). In order to understand this professional code, a concrete definition of ethics must be obtained. Ethics is "the study of good and bad conduct within a profession."[14] The International Foundation for Protection Officers (1999) gives an example of a code of ethics for security officers:

1. Respond to employer's professional needs
2. Exhibit exemplary conduct
3. Protect confidential information
4. Maintain a safe and secure work place
5. Dress to create professionalism
6. Enforce all lawful rules and regulations
7. Encourage liaison with public officers
8. Develop good rapport within the profession
9. Strive to attain professional competence
10. Encourage high standards of officer ethics (p. XXI)

Security officers who follow this code of ethics are true professionals at their profession.

Professionals have both duties and obligations, combined with morality, which are congruent with the ethics of a certain profession. The definition of duty must also be examined in order to come to a better understanding. A duty is "a professional obligation to do a certain thing" which can be established or changed by statute, custom, or contract of the employee. Professional employees "think in terms of their duties and obligations, not their authority."[15] When examining a professional employee, there are also certain attributes that compliment his or her personality. Some of these qualities include honesty, sincerity, integrity, helpfulness, and loyalty.

"A true professional has the following:

- Education relating to the profession.
- Training for the tasks and duties that must be performed.
- Experience within the profession
- A commitment to the profession marked by continuously striving for excellence"[16]

In addition to much commitment and education in the employee's specific field, a professional employee must also be conscious and professional in his/her deportment. Deportment is defined as how one carries oneself and the image and attitude that is portrayed by the employee's appearance.[17] Professional employees keep in mind that when dressing, one is a representative of his/her employer and/or client. Professional employees realize that the public judges an employee sometimes only by physical appearance; therefore, an employee being sharply dressed, cleanly shaved, and neatly groomed hair would portray an

---

13 D. June (1999). *Introduction to Executive Protection*. Washington, DC: CRC Press, p. 252.

14 C. Hertig (1998). Ethics and Pdrofessionalism In *Protection Officers Training Manual*. Woburn, MA: Butterworth-Heinemann, p. 274.

15 Hertig, p. 274

16 Hertig, p. 274

17 Hertig, p. 274–76

image of a professional to the public. Along with deportment, professional employees must comport themselves with manners, which are "simply accepted means of conducting oneself in public."[18] Politeness, consideration, and respect for others are all manners that professional employees would possess. Overall, a professional employee contains both internal and external qualities that classify him/her as a professional employee.

Unfortunately, while all security supervisors wish that every protection officer carried the attributes of a professional employee, there are many officers that contain attributes of a problem employee as well.

The Problem Employee

A problem employee is one who disrupts the normal flow of activity in a workplace. This type of employee could either be well liked by other employees as a "class-clown," or be disliked by other employees as a problem maker. However, for the most part, a problem employee is the cause of much distress for both other employees and the supervisor.

Some violations specific to the workplace may include break policies, uniform policies, safety regulations, and smoking policies. Human nature is very unpredictable, and therefore it is impossible to state every single violation a problem employee might engage in. However, the three main areas in which most employee problems occur are attendance, behavior, and performance.[19] Any employee containing an unacceptable attendance rate, engaging in inappropriate behavior, or performing unsuitably would be considered a problem employee. There are many attributes that would also describe a problem employee. Some of these attributes include dishonesty, negligence, carelessness, and the presence of unnecessary emotions. "Anger, lust and greed devastate good people and destroy great organizations."[20] Problem employees not only disturb the people around them but also the organization itself. Protection officers must not allow themselves to fall into this category of employees. If an officer engages in problem behavior, he or she must realize that the supervisor can impose disciplinary measures.

The Disciplinary Process

The whole disciplinary process should contain two steps. The violations must be detected and corrective action must be taken.[21] Managers, when disciplining subordinates, should ask themselves "whether subordinates can learn from their mistakes. If they can, using discipline to teach rather than to punish is both more humane and better from a business viewpoint."[22] The manager must view the subordinate as an individual and deal with them on that basis. This will ensure loyalty and support from the subordinate, regardless of the disciplinary actions taken, and will motivate the subordinate to succeed.[23] The entire disciplinary process can be explained with six rules, devised by Charles Sennewald in his book, *Effective Security Management*. They are:

1. All rules are to be documented. No unwritten rules.
2. If you must discipline a subordinate, do it privately.
3. Don't get personal/Don't play favorites. Treat employees in a fair and equal manner.
4. Don't embarrass them, teach them. Behavioral change, not deliberate humiliation, is the key.

---

[18] Hertig, p. 275

[19] J. D. Levesque (1986). *Manual of Personnel Policies, Procedures, and Operations*. Englewood Cliffs, NJ: Prentice Hall.

[20] N. E. Trautman (1999). Unethical Acts by Security Officers. In *Security Supervision: Theory and Practice of Asset Protection*. Woburn, MA: Butterworth-Heinemann, p. 76.

[21] Stone, p. 350

[22] Burstein, p. 72

[23] C. A. Sennewald (1985). *Effective Security Management*. Boston, MA: Butterworth Publishers, p. 108.

5. Keep track of infractions. This provides support for more drastic disciplinary actions if the employee is a chronic offender.
6. Be prompt. Don't wait. If there is a violation, correct it immediately or as soon as possible.[24]

Disciplinary Policy

If an employer intends to utilize disciplinary procedures, it is a good idea for the management of that company to write a disciplinary policy. This policy can be clearly explained in the company's handbook or employee orientation sessions, posted by the time clock or break room, or other ways. If the employees know the disciplinary policies and procedures, they will know what will happen to them if disciplinary action is ever taken, and what is expected of the employee. The following are a few guidelines that a disciplinary policy should include:

1. Explanation of rights: This is a statement that would inform the employee that the employer has the right to change or modify the policy as they deem necessary, depending on the situation. This statement would not allow the employer to ignore the policy, but it will let the employee know that certain circumstances will be handled differently than others. Circumstances may be based on the number of offenses, frequency, and severity.
2. Knowledge of penalties: It is important for a supervisor to know what action should be taken to discipline an employee, whether it is docking of pay, suspension, legal action, etc. If an employee is caught stealing a box of pens, the penalty will probably be different than the penalty for stealing a desktop computer. If investigation revealed that the same employee had been stealing a box of pens every Monday for the last 6 months, then the penalty would again change. Although they are still stealing the same item, the dollar amount for the loss to the company would be higher, thus the penalty more severe.
3. Standard operating procedure: Most organizations have some sort of SOP (standard operating procedure) manual outlining how the organization is to operate. A section on employee discipline must be included. An organization's SOP should have a code of conduct that employees are required to follow, along with an outline of disciplinary action for various types of infractions. One must accurately plan out a step-by-step procedure that will be the most efficient to utilize, while keeping the disruptions in the organization to a minimum.
4. Efficiency: All disciplinary action should be dealt with in a swift, yet fair manner. The employee must have a chance to defend him- or herself before a decision is made. Therefore, action cannot be delayed. It is important to remember that the violator is still "on the job" while the supervisor decides what, if anything, to do. In some cases, the longer the delay, the greater the difficulties for management when action is finally taken, or if an injured party objects to the delay. Theft cases are fairly straightforward, but a case where sexual harassment is involved becomes much more complicated, especially if the victim seeks legal restitution. This can be harmful both for the employees *and* the public image of the company. If both parties see that the matter is being handled as quickly and quietly as possible, then the need for legal counsel by the outside parties could be avoided.

When to Enforce Disciplinary Policy

One of the most important things a supervisor must know is *when* disciplinary action is necessary. There are several times when disciplinary action is an appropriate corrective action. Examples of these are:

- Excessive tardiness
- Defective workmanship

---

[24] Sennewald, p. 111–12

- Inadequate work performance
- Poor attitudes that affect morale
- Insubordination[25]

These infractions, except for insubordination, are common and can be found in virtually every workplace. Insubordination, as defined in *Black's Law Dictionary*, is:

> *State of being insubordinate; disobedience to constituted authority. Refusal to obey some order which a superior officer is entitled to give and have obeyed. Term imports a "wilful" or intentional disregard of the lawful and reasonable instructions of the employer.*[26]

These violations, as compared to criminal law, are *mala in se*. Other violations, or the rules enacted by particular companies for particular reasons, may include break policies, uniform policies, safety regulations, smoking policies, etc. These are the *mala prohibitum* crimes of the workplace.

Determining the Necessity of Disciplinary Action

In order to determine if a violation has occurred, the event/incident must be *investigated*. The investigative process can be broken down into seven items. They are:

1. What happened? Is there any physical evidence?
2. Is the infraction serious? Major or minor? How many people are involved?
3. Was the violator aware of the rule that was broken? Did the violator have a "reasonable excuse"? Are there any aggravating or mitigating circumstances?
4. Does the violator have a record of such conduct?
5. Should the violator receive the same treatment as others for the same offense? Different treatment?
6. Was the offense documented?
7. How can the problem be prevented?[27]

A supervisor must also look at the following when investigating an infraction:

1. Frequency/nature of problem: Is this a continuing occurrence? Is this rule broken repeatedly by the same individuals?
2. Employee's work history: How long has the violator been employed? Does the violator perform quality work? A good way to look at work history would be to remember: the longer the tenure, the lesser the discipline.
3. Degree of socialization: How has management made the employee aware of rules and regulations? Are they written? Informal?
4. Organizational discipline practices: How was this infraction dealt with at other times/with other employees? Is management consistent?
5. Implications for coworkers: Could disciplinary action against one employee interfere with the morale of the rest?
6. Management backing: Can the supervisor justify how and why a person was disciplined?[28]

---

[25] R. M. Hodgetts (1987). Effective Supervision: A Practical Approach. NY: McGraw-Hill, p. 358.
[26] H. C. Black (1990). *Black's Law Dictionary*. MN: West Publishing Co., p. 801.
[27] Hodgetts, p. 359
[28] Robbins, p. 396–97

There are also some important factors that employers have to consider when deciding on discipline. Darrel Stephens provides five factors that employers should consider when disciplining a protection officer:

1. Employee motivation: Was the employee acting in the best interest of the business or the public?
2. Degree of harm: Harm can be measured by monetary costs to the department and the community, personal injury, and reputation of the business.
3. Employee experience: Was the employee a new employee or an experienced employee?
4. Intentional and unintentional errors: Was the error intentional or unintentional?
5. Employee's past record: Is this the first incident of misconduct?[29]

Discipline Methods

After a supervisor has investigated an infraction or complaint, and determined it to be true, it is time for that supervisor to take action to *correct* the situation. Notice the emphasis on the word *correct*. Although disciplinary action is a punishment, its goal is to change a behavior, not to merely acknowledge its occurrence.

> *Any punishment connected with discipline should always be a means to an end, and that end should be organizational, not personal.*[30]

There are six ways to discipline an employee. Five of them are listed here, in order of severity:

1. Oral warning: The supervisor explains the violation and the seriousness of it to the employee. The supervisor should allow the employee to react to the warning and then permit the employee to ask questions. The warning must also include the required improvement in behavior, and mention assistance that may be provided by the supervisor or the employer. The penalty, if there is one, should be stated clearly. These warnings should be documented and placed in the employee's personnel file.
2. Written warning: The procedures are the same for written warnings as for oral ones, but the written warning is used for repeated or more serious infractions, where the oral warning is not. The written warning should be in the form of a letter to the employee, and should be written in a "punitive" tone. A copy of this letter should be kept in the employee's personnel file.
3. Suspension: This action is used only after repeated written warnings or for serious infractions that may not warrant dismissal from employment. Suspensions may also be used if "an unfortunate incident of misconduct on the job requires temporary removal of the employee from the work environment, or where doubt about guilt in some instance necessitates a period of investigation."[31] Like the written warning, a letter should be written to the employee stating the reason for the suspension and its duration. A copy of this letter should be kept in the employee's personnel file.
4. Pay cut: This method, though infrequently used, is basically a reduction in an employee's salary or hourly wage, either temporary or permanent. This method is demoralizing to the employee and defeats the purpose of using discipline as a *corrective* measure. These actions should be documented and placed in the employee's personnel file.

---

[29] D. W. Stephens (1994). Discipline philosophy. In FBI Law Enforcement Bulletin, Vol. 63, Issue 3, Washington, DC, p. 21–22.

[30] Sennewald, p. 107

[31] Stahl, p. 311

5. Demotion: This method, like the pay cut, is demoralizing to the employee *and* his coworkers. Demotion is used as an "attention getter" by management and is reserved for tenured employees or those perceived by management as "not easily fired." These actions should be documented and placed in the employee's personnel file.[32]

Dismissal: The "Sixth" Disciplinary Method

This method should be used *only after* all other avenues have been exhausted. The power to dismiss an employee is generally not held by a first- or second-line supervisor, but by upper management. Some supervisors do have this power, but it is in their best interest to confer with upper management prior to dismissing an employee. A letter should be sent to the employee advising them of the dismissal, and a copy of this letter should be kept in the former employee's personnel file.[33]

Dismissing a subordinate should be the "last resort" of the disciplinary process. It is an important determination that requires accurate information to support the decision. A supervisor/manager must determine what reasons they have for dismissing an employee, and if the employee's record warrants this decision. Documentation of all actions that have been taken in prior instances against the employee must be kept to protect the employer in case of legal action. Mary A. DeVries, in her book, *The Complete Office Handbook* suggests:

1. Tell the person why they are being dismissed, and do not make excuses or apologies or appear in any way to be indecisive or unsure of the decision to dismiss.
2. State the case calmly and unemotionally, using the documentation that has been developed.
3. Do not engage in a debate or respond to emotional accusations. Simply state the facts and try to focus the discussion on severance conditions.
4. If you believe the employee will persist in a debate or become hostile, hold the meeting outside the office in a place where there is more than one exit.
5. Do not attempt to stop or dissuade the person from working out a new professional life elsewhere.
6. Offer to accept a letter of resignation from the employee and work out an agreeable announcement to coworkers and outsiders.[34]

The Appeals Process

If employees are going to be disciplined, there should exist a way to appeal for the actions taken against them. Although supervisors generally have experience in their field and have demonstrable leadership qualities, they are not perfect. If they were perfect, there would be no employees—just supervisors. Some supervisors do use their disciplinary powers for personal reasons.

Hearings are generally used for more severe actions; a verbal or written warning should not justify an appeal. Suspensions, demotions, and dismissals are arenas in which appeals occur. Appeals should be "heard by a multiple body—often of three persons—which is established by statute or which is appointed ad hoc by the head of the department."[35] The appeal "board" should be as objective and as unbiased as possible. When possible, appeal "boards" should be composed of employees outside the department, and it is better if they are of supervisory rank or higher. If the department is unionized, have a union representative present or even allow one to sit on the appeal "board." This way, there can be no valid accusations that the decisions of the appeal "board" are unfair.

---

[32] B. Keys and J. Henshall (1984). *Supervision*. NY: John Wiley & Sons, p. 274–75.

[33] Keys and Henshall, p. 274–75

[34] M. A. DeVries (1987). *The Complete Office Handbook*. Avenel, NJ: Wings Books, p. 32.

[35] Stahl, p. 315

Low Employee Morale

Sometimes, employees do things that warrant disciplinary action for reasons other than personal gain or poor decision-making skills. "Low employee morale" is the culprit when these types of offenses start occurring, and morale becomes low for a number of reasons. In these cases, sometimes the best way to change employees' behavior is not to discipline them, but to work with them to correct situations that cause low morale. Here are a few examples:

- Poor working conditions
- Poor equipment
- Lack of communication
- Hypocrisy
- Redundancy

When employees work in a poor environment, their morale is lowered because they wish that conditions were better. Who would want to work in an environment that makes a person feel like there is no way out? This might lead an employee to adopt poor work habits and methods, which may warrant disciplinary action. Supervisors and managers should bear in mind that if *they* would not like working in an environment, other people probably wouldn't either. If the manager's office has carpeting, comfortable chairs, a large finished wooden desk, leather couches, and an advanced phone/computer system, the employees' morale will most likely be lowered if they have old metal chairs and 20-year-old desks, cold tile floors, inadequate lighting, no couches, rotary phones, and typewriters. An employer should provide a comfortable workplace for employees in order for them to work more efficiently.

Having poor equipment also can have an effect on employees' actions. For example, a security department has a poor two-way radio system. A patrol officer attempts to call the supervisor via radio, but does not get a response. The officer tries again, and again, no response. Then the officer goes to a phone and calls the supervisor. The officer informs the supervisor of the radio difficulties and conveys the message that he or she was originally trying to send. That officer may then decide not to patrol as often due to the safety hazard of not having reliable communications with backup officers. If this officer is not patrolling as he/she should be, then that officer is neglecting his or her duties. The supervisor, caring only that patrols are being performed properly, may take disciplinary action against that officer, regardless of the circumstances. To discipline an officer while ignoring circumstances such as these would be unfair to that officer and to the organization. A better alternative would be to discuss the problem with the officer and determine ways to enhance radio performance.

Lack of communication within the organization can also lower morale. The employees might feel like they are "out of the loop," and feel uninformed about certain issues, such as policy changes and other important announcements. A system should be set up to make sure that *all* employees are made aware of new information that affects their job requirements. A chain of command can be used, an email list can be set up, or something as simple as typing or writing a memo can ensure everyone knows what is going on. A sign on the wall or writing information on a bulletin board is not good by itself because people may not notice it. Employees who are away from work for some reason (whether they are on vacation, taking a personal day, attending job training, etc.) will not be in the area where the information is posted. If everyone knows what is going on, the organization can operate more smoothly.

Hypocrisy in a workplace is another big issue that can commonly be overlooked. If a policy is written, it should be followed by everyone. On the same token, the policy should be enforced by all of the supervisor/managers. If a security supervisor allows one officer to "bend the rules," but another supervisor does not allow this and disciplines that officer, that will also cause problems, particularly within the department. The disciplined employee will point this out to management if he/she appeals the disciplinary action. Management is then faced with deciding *who* needs to be disciplined, as well as why.

Finally, redundancy is probably the most overlooked cause of low worker morale. In other words, a routine is established. If employees do the same thing each day, they tend to lose interest and get bored, leading to the development of poor work habits. Tardiness is one

result of redundancy. In most cases, however, this cannot be avoided. A supervisor/manager generally cannot alter the employee's duties so that they are more "exciting." What they can do is add a little something positive to the standard, everyday routine. Buying lunch for the department periodically, holiday parties, and an "Employee of the Month" award are all ways a supervisor/manager can help boost morale. It will give the employees an opportunity to socialize with each other in a more social atmosphere, rather than in a working atmosphere. It can also be viewed by the employees as sort of a "thank you" from upper management, that they are doing a good job, and are appreciated.

Ten Commandments of Discipline

In addition to the guidelines, the Ten Commandments of Discipline may further help supervisors understand and effectively enforce discipline. These Ten Commandments should be used as a bible for any supervisor who is faced with the possibility of disciplining a protection officer.

1. Understand the five personality types of employees to help reduce the need for discipline: A supervisor who understands the five personality types will be able to assign work to officers that will satisfy their personality type; therefore, supervisors will gain the officer's compliance and will reduce the need for discipline.
2. Evaluate the situation in its entirety: Supervisors must get all the facts before an officer can be disciplined. Get information from the officer who engaged in a violating behavior as well as other employees in the area who saw the situation. If there are security cameras in the area, view the tapes to gain physical evidence.
3. Make sure the policy the officer violated is written clearly and concise: A supervisor cannot discipline an officer over a poorly written and very confusing policy. Similarly, the discipline given must be thoroughly documented.
4. Explain to the officer why his or her actions violate company policy and why discipline is necessary: It is very important for the officer to understand why his or her actions were wrong. This will help the officer learn not to do it again in the future.
5. Pick a disciplinary method that is fair and just: The phrase "let the punishment fit the crime" can be used here. Look at past situations that were very similar and see what disciplinary action was used. Make sure the disciplinary method is appropriate to the violating act.
6. Job termination should only be used as a last resort or when all hope of effective discipline has failed.
7. Make sure the discipline is engaged in a swift manner: Do not procrastinate or take a long time to decide on the disciplinary action. The discipline will lose its potency if not given in a swift fashion.
8. Do not discipline when angered or upset: The situation the officer engaged in may upset a supervisor. Allow time to cool down and relax. This will help a supervisor make good judgmental decisions on the appropriate disciplinary action.
9. Do not hold a grudge against the officer: Protection officers will make mistakes and need to be disciplined; however, once the discipline is complete, do not look down at the officer because of his or her previous action. Believe that the officer has learned his or her lesson and is ready to move on and be a productive part of the organization.
10. Understand that there should be an existing way for the officer to appeal the discipline if he or she disagrees with the method of discipline or the disciplinary process the supervisor engaged in: Most companies have some kind of appeals process whether it would be a review board, human resources department, or even management. Do not deny the officer this opportunity. Supervisors can make bias decisions without even knowing it. This is a good way to check that supervisors handle the situation in a correct manner.

Supervisors who follow these Ten Commandments will make better disciplinary decisions and gain the compliance and obedience of the protection officers, therefore, helping the organization to become more productive.

Employee Discipline: Policy and Practice Quiz Questions

1. Discipline is basically an action taken by a supervisor to correct the behavior(s) of a subordinate employee, generally within that supervisor's department. ☐ T ☐ F
2. Discipline is usually prompted when a mistake is made, often in the form of a _____.
3. Possible reasons to enforce disciplinary policy may include:
   a) Excessive tardiness
   b) Defective workmanship
   c) Inadequate work performance
   d) All of the above
4. In order to determine if a violation has occurred, the event/incident must be _____ .
5. Although disciplinary action is a punishment, its goal is to change a behavior, not to merely acknowledge its occurrence. ☐ T ☐ F
6. List six ways to discipline an employee:
   a) _____
   b) _____
   c) _____
   d) _____
   e) _____
   f) _____
7. The power to dismiss an employee is always held by a first-line supervisor. ☐ T ☐ F
8. _____ in a workplace is another big issue that is commonly overlooked.
9. If an employer intends to utilize disciplinary procedures, it is a good idea for the management of that company to write a disciplinary policy. ☐ T ☐ F
10. The following are a few guidelines for what a disciplinary policy should include: (select best answer).
    a) Explanation of Rights
    b) Knowledge of Penalties
    c) Standard Operating Procedure
    d) Efficiency
    e) All of the above

This page intentionally left blank

7 Human Reliability

Martin Hershkowitz

Introduction

Violence in the workplace is one of today's greatest management fears. The inability to predict and therefore avoid a violent incident caused by an employee or visitor is a frustration that few managers can successfully cope with since needed protection measures may violate the individual's civil rights. This situation can reach nightmarish proportions when the instrument of protection, the armed security officer, becomes the violent employee. Here is an individual who is trained in the arts and sciences of violence, and carries the weapons of violence with him or her into the workplace.

Fortunately, security management can rely on the principle of "compelling need" to develop protective measures against the likelihood that the security officer becomes the violent employee. When the workplace is a nuclear weapons plant, a nuclear power plant, an explosives production plant, or a corrosive chemical plant, the violent act and resulting damage could reach catastrophic proportions and the compelling need for human reliability is quite clear. Under such situations, the compelling need to utilize protective measures that may impact on the individual's civil rights in order to protect the health and welfare of all employees, the employer, and the general public becomes the major concern. As the potential for a catastrophic situation decreases, the compelling need decreases more rapidly. Security management, nevertheless, must apply proactive activities that will assure that the security officer displays "good judgment" on the job.

Defining Good Judgment

What does the term "good judgment" mean? A simple operational definition is that the employee makes rational decisions in accordance with accepted operational procedures and carries them out in an acceptable manner—regardless of the momentary conditions of the job or the frustrations from personal, family, social, and/or financial difficulties. Since some conditions of the job and some personal situations can be overwhelming, the ability to display good judgment becomes an extremely important characteristic.

Assuring Good Judgment: A Human Reliability Program

Security management can assure continuing good judgment of its employees through an integrated human reliability program (HRP). An HRP is composed of regular medical examinations and evaluations, psychological evaluations, drug-use testing, alcohol-dependency testing, training in peer behavioral observations, national and local criminal record checks, financial stability investigation, and an integrated employee assistance program. Depending on the demonstration of compelling need, some of these HRP elements may be considered to be a violation of the individual's civil rights; however, for purposes of this discussion each element will be reviewed herein.

Background Review

The most common way to determine if an individual will display continuing good judgment is to determine if the individual has displayed that good judgment in the past. It follows that a comprehensive preemployment screening and analysis, including national and local criminal record checks, a credit check, and indicators of spousal or child abuse provides valuable information for determining "human reliability." Prior employment and social contacts should be personally interviewed to determine indicators of judgment that are unacceptable in the workplace. For current employees, the comprehensive screening and analysis should be repeated as a periodic background review, once every year or two.

Although this activity is well defined, it requires professional adjudicators to ensure that the analysis of information leads to a clear determination that the individual has displayed good judgment in the past and will continue to display good judgment in the future. This is true for both preemployment screening and periodic background review.

Medical Examination and Evaluation

Medical evaluation is a complex undertaking as the individual being examined and evaluated is not the physician's patient as is traditionally the case. The Occupational Medical Physician works for the organization; therefore, the physician is responsible for determining if the individual is both "fit for duty," which traditional medical training equips the physician for, and "displays good judgment," which is not part of the traditional medical training. The former seeks to determine if the individual is physically capable of carrying out the duties of the job. The latter seeks to determine if the individual is mentally and emotionally prepared for the rigors of the job. However, the provisions of the "Americans with Disabilities Act of 1990" may have some legal impact on this.

The Occupational Medical Program should require both a preemployment and regular periodic medical examination by a physician trained in occupational medicine who will seek indicators of illegal drug use, prescription drug abuse, and/or alcohol dependency; medical limitations on fitness for duty; and the existence of other disqualifying conditions. Finally, the Occupational Medical Director should be able to integrate these results with the findings from other HRP elements and issue a medical statement that there are no existing medical or psychological conditions that could lead to a display of poor judgment in the workplace or that the individual is not or is no longer able to perform in this position.

Drug Testing

Drug testing is not a simple concept. To begin with, drug testing cannot be conducted on a regular, published schedule. In order to be effective, drug testing must be conducted during the preemployment interview and through 100% random sampling of the workforce (so that every employee is tested at least once during every testing cycle). To ensure that the results are accurate and that the individual's civil rights are not violated, it is necessary to conduct the drug testing through a three-step process with a rigorous "chain-of-custody" to guarantee evidential purity.

The first step is a screening test to determine if there is an indication of possible drug use. The most commonly accepted screening process is the radioimmunoassay using approved thresholds to establish a presumed positive. Each drug has an approved reading threshold, below which the sample is said to be free of the drug. If the sample yields a reading above the threshold, the sample is said to be a presumed positive. Presumed positive should not be mistaken for positive. It is merely an indicator of the need to perform a confirmatory test.

The second step is the confirmatory test to determine if there was in fact a positive finding of drug use. The preferred confirmatory process is the gas chromatography/mass spectrometry (GC/MS) using approved thresholds to establish a confirmed positive. As with the screening process, a reading below the threshold is taken to be a confirmation that there was no drug use; a reading above the threshold is a positive finding of drug use.

In both steps, a rigorous chain-of-custody must be guaranteed or the evidence is tainted and of no value. To repeat the process(es) at this point is of little value as the

individual has had sufficient time to cover any drug use through a variety of available techniques.

The third and final step is a review of the drug test results by a Medical Review Officer, a physician who is trained to determine if the positive reading is a result of actual drug use, cross readings from the use of prescribed drugs, or the accidental ingestion of material that can result in a false positive. If indicated, the Medical Review Officer may interview the employee to determine the reason for the positive reading.

Psychological Assessment

Psychological assessment results from a two-part process consisting of psychological tests to establish and periodically update a baseline and regular psychological interviews to determine if the individual is beginning to display behavioral problems. This assessment is incorporated into the medical evaluation to provide a complete picture of the individual's ability to display good judgment on the job.

Psychological tests and accompanying interviews are designed to meet a variety of needs. HRP psychological assessments are not designed to determine mental illness as it may or may not be a factor in displaying good judgment; mental illness may be related to "fitness-for-duty," which is a different issue. At the other end of the scale, HRP psychological assessments are not designed to determine fraud or petty theft, which is likewise a different issue. HRP psychological assessments are designed to detect an employee's gradual emotional deterioration due to personal and/or job related stress and an applicant's inability to display good judgment due to psychopathology.

The preferred psychopathological test is the Minnesota Multiphasic Personality Index II (MMPI-II). Although this test has not been adequately tested in the courts, it is a revision of the original MMPI, which has been tested and found to be legally valid. Another psychopathological test is the Millon Clinical Multiaxial Inventory (MCMI), but this test has not been sufficiently tested in the courts to be used alone. A third test of some interest is the Sixteen Personality Factors (16PF); however, this test is used more to differentiate personalities and is not considered to be a psychopathological test.

There are many types of psychologists who are proficient in performing a psychological assessment; however, the HRP psychological assessment should require a clinical psychologist. The clinical psychologist is trained to detect psychopathological tendencies and to interpret the ability to display good judgment in the workplace.

Alcohol Dependency

Alcohol abuse takes two forms: acute alcoholism, which is typified by the employee who reports to work drunk, and chronic alcoholism, which describes the individual who is a habitual and excessive user of alcohol. Both forms are a threat in the workplace as they affect both judgment and reaction time. Normally, acute alcoholism in the workplace is taken care of through behavior in the workplace rules; that is, show up drunk and you don't work! In addition to the loss of a day's pay, there may be other penalties according to those rules.

Chronic alcoholism affects the thought processes and judgmental reasoning to such an extent that the individual becomes a danger to himself or herself and begins to display very poor judgment in the workplace. Due to the nature of this problem, an alcohol-dependence testing program must be established for the security officers. Similarly to the drug testing program, alcohol testing should be conducted during the initial interview and through a 100% random sampling of the workforce (so that every employee is tested at least once during every testing cycle).

The alcohol-dependency testing program should contain the following requirements for testing purposes: during the initial interview or prescreening; during the periodic medical examination; under a random testing procedure; for cause (that is, the employee exhibits signs of being under the influence of alcohol); and after accidents and/or mortal injuries.

The testing program can include one or more of the three common tests for alcohol use; blood test, urine test, or breath analysis. Of the three, breath analysis is the most effective and least invasive, thus more acceptable.

Recognition of Behavioral Change or the Display of Unusual Behavior

Behavioral change or unusual behavior is simply defined to be any change from the way a person usually behaves. Such changes do not have to be permanent to indicate the potential for deteriorating judgment, but they do need to be recognized. In most working relationships, a fellow worker or immediate supervisor is in an excellent position to detect such changes. The problem is how to tell when that change is due to some momentary lapse in good judgment and when it is an indicator of a serious deteriorating condition.

All employees and supervisors need to be trained both to recognize behavioral change, including stress, environmental pressures, and depression, and to report positive observations to the Occupational Medical Director for further investigation, counseling, and treatment. This is not a "snitch" program. Serious behavioral change is a major indicator of a potential deteriorating condition. The employee exhibiting this change in behavior may be about to commit a violent and catastrophic act.

The training program should include the following on-the-job behaviors and work habits that directly impact efficiency, effectiveness, and good judgment: change in work quality or quantity, increase in mistakes or bad judgment, decrease in efficiency, difficulty in concentrating, absence from the job, absence "on-the-job," ignoring company policy, becoming overcautious, becoming overzealous, increase in risk taking, increase in accidents, and change in cooperation with coworkers. In addition, concern over the employee's change in work relationships and social interactions should be part of the training program.

Integrated Evaluation by Management

A simple caution should be observed at this point. All the tests and assessments discussed above are isolated events. A decision made based strictly on one of these data points is likely to be a wrong one. The decision must be based on an integrated review of all results. In particular, the report by the Occupational Medical Director has already integrated many of the tests and assessments and should be considered very carefully; however, the background review is of great importance and should be considered with equal weight. Only the security manager is in a position to integrate all this information and make the vital decision on hiring the applicant or assigning the employee.

Employee Assistance Program

Thus far, the discussion has concentrated on testing the applicant and employee. Unless the organization is prepared to assist the employee to overcome his or her difficulties, all that has been accomplished is that well and expensively trained security officers will be underused or discharged. This is a poor use of organizational resources. A much better use of those resources is to establish an integrated employee assistance program, where the employee is helped to overcome the medical, health, social, and/or financial problem.

It is important that the employee assistance program be sensitive to the security aspects of the employee's duties. A program that ignores this aspect and conceals the employee's problems and deteriorating good judgment is counterproductive to the organization's needs. By integrating this effort into the HRP, security will be retained at a high level of effectiveness.

Security Management Responsibilities

There are three levels of security management: the security executive, the security manager, and the security supervisor. In the real world, the responsibilities, functions, and duties of these three levels are not mutually exclusive. There are real and perceived overlaps and occasional gaps; however, for the purpose of this discussion consider that they are mutually exclusive.

The Security Executive

The security executive is primarily concerned with policy, strategic planning, growth, legal issues, and profit. With regard to the HRP, the security executive is mostly concerned with establishing,

through the corporate counsel, the level of compelling need and with determining, through the comptroller, the number and extent of HRP components to implement in order to get the "most bang for the buck." The security executive is interested in the protection that an HRP can offer to reduce the risk of a catastrophic event occurring due to a security officer displaying bad judgment, but is not interested in paying any more than necessary to achieve that goal.

The Security Manager

The security manager is primarily concerned with operational issues, such as program planning and shift scheduling; identifying, clearing, hiring, and training security officers; identifying and hiring an Occupational Medical Director, Occupational Medical Physician(s), and clinical psychologist(s); contracting with a certified laboratory to conduct screening and confirmatory tests for substance use/abuse (both drugs and alcohol), with the required chain-of-custody control; establishing or contracting for a training unit, to include peer behavioral change observation training; establishing or contracting for an employee assistance program; and establishing an integrated management evaluation team. The security manager has the responsibility for establishing the HRP and making it work properly under the constraints placed on it by the security executive, but only from a programmatic perspective, with an emphasis on operating costs, time management, and minimum disruption to shift schedules.

The Security Supervisor

The security supervisor is where "the rubber meets the road." The security supervisor deals with the human being inside the uniform, the individual who might be experiencing deteriorating judgment. The security supervisor has the responsibility for setting the schedules; for ensuring that the security officer attends all trainings, provides all the necessary samples, and visits the physician and psychologist; for observing any significant changes in behavior that would warrant medical and psychological evaluation; and for ensuring that the security officer anonymously received the full value of an employee assistance program. The single most important principle governing the relationship between the security supervisor and the security officer under the HRP is that "no one gets a free pass"; the security officer cannot know in advance the date of the drug and alcohol tests, cannot miss medical and psychological evaluation appointments, cannot miss important training dates, cannot miss appointments with the employee assistance program.

Conclusion

Violence in the workplace is real and increasing rapidly. Although this is not the reason why large, well-trained security forces exist, it is clearly a benefit that fellow employees, shoppers, students, hospital patients, and the general public appreciate. However, when a member of the security force, someone who is well trained in the use of violence and who brings those tools of violence into the workplace, begins to display deteriorating judgment, the level of concern becomes intense. It is for this reason that there may be a compelling need to require that security officers submit to tests and procedures that have a very high likelihood of providing foreseeability of workplace violence.

The collection of tests and procedures are traditionally called an HRP, but has been known by other names as well. The components of the HRP are as follows:

1. Background review
2. Medical examination and evaluation
3. Drug testing
4. Psychological assessment
5. Alcohol dependency
6. Recognition of behavioral change or the display of unusual behavior
7. Integrated evaluation by management
8. Employee assistance program

The use of the HRP does not guarantee that the security officer's good judgment will not deteriorate, but it does assure that the early signs of deterioration will be detected and that the security officer who no longer can display good judgment will be removed from the workplace until the problem can be addressed and corrected. In this manner, the on-duty security force is assured to display continuing good judgment.

Human Reliability

Quiz

1. Medical _____ is a complex undertaking as the individual being examined and evaluated is not the physician's patient.
2. Psychological _____ results from a two-part process consisting of psychological tests.
3. Drug testing cannot be conducted on a _____ schedule.
4. Alcohol abuse takes two forms: _____ alcoholism and chronic alcoholism.
5. There are three levels of _____ management.
6. Violence in the workplace is one of today's greatest management fears.
   ☐ T ☐ F
7. A drug test presumed positive normally necessitates termination of an employee.
   ☐ T ☐ F
8. Every Organizational Occupational Medical Program makes it compulsory for a pre-employment medical examination.
   ☐ T ☐ F
9. Alcohol abuse takes two forms: Acute alcoholism, which is typified by the employee who reports to work drunk, and chronic alcoholism, which describes the individual who is a habitual and excessive user of alcohol.
   ☐ T ☐ F
10. The collection of tests and procedures are traditionally called a Human Reliability Program (HRP).
    ☐ T ☐ F

UNIT

III

Supervision

This page intentionally left blank

1 Personnel Deployment

Inge Sebyan Black

The Right Fit

Having the right individual in the right position is a profound statement. It may make the difference between a lawsuit, keeping a client, or saving a life. It could be said that any one of these make it one of the most critical decisions you will have to make. Your decision also has a direct impact on the bottom line for you and your client since the right fit will have a positive effect on scheduling, client satisfaction, retention, and increased effectiveness.

Maximizing personnel is about looking at the position that needs to be filled and then finding the right person to fill that position.

Information Gathering

To assist you in your decision you will want to look at a number of elements:

1. Duties and responsibilities required
   These need to be clearly stated. Understand the qualifications and/or level of training required to perform efficiently. Will they need to be certified in CPR, Automated External Defibrillator (AED) or first aid? How proficient will they need to be to utilize the closed circuit television (CCTV), security system, fire system, or access control? Will they be the Information Technology (IT) administrator? Will they fully understand the requirements of the position? Will they need to greet customers? Will they be driving a vehicle?
2. Specific officer skills and training
   Does the officer have a specific skill set, that is, emergency training, technical training, firearm training, patrol car training, or state mandated training? Evaluate the character of the officer. Is he honest, courageous, alert, well disciplined, ethical, and loyal? There are a number of interviewing methods to determine a character of a person. Some are through paper and pencil tests, others through situational questions. It is important that whatever tools you use to evaluate your officers, you remain consistent with all of your staff. Do not single out a staff member for testing.
3. Full understanding of staffing
   Is the position temporary or long term? Is it full time or part time? Will the shifts be rotating or shift work? Is the post a foot patrol, vehicle patrol, or stationary? You will want to evaluate the position and determine factors. How many weekends will each officer need to work?
4. Information gathering
   Since security is often a 24-hour a day, seven days a week profession, gathering information will be critical in effective scheduling and deployment, as well as recruitment. It will be important to fully understand the needs of the specific position and the skill set of the individuals you have or will have to recruit. You can gain information through interviewing the client, listening to the client, observation, and/or using a questionnaire.

Recruitment

Whether you do the recruitment or you have someone on your staff who assumes that responsibility, you will want to understand staffing, the specific procedures, testing, training, and the hiring process. The information you gathered from your client, along with the parameters of the job description, will assist you with the right choices. Your knowledge of the client, post orders, job site, and other key factors will help you match a candidate with the job duties and the client.

The important element is matching that right person for the right job. It may not always be necessary to obtain a superstar because of the many demands made upon them and the knowledge they must possess. Therefore the job description must be broad enough so that the most talented apply and those with less talent will still be considered.

Interviewing is the skill needed to successfully find that right person. Interviewing is a subject that is very involved and should be done by someone with experience and training. Your company may have a Human Resource department (HR) to do the hiring and interviewing but even if you do have, an HR department you may be the one to make the final selection. By the time you interview the person, you will be able to address questions specific to the job and officer, therefore, deciding if it is a good match.

Scheduling

Scheduling can definitely be challenging when you are dealing with real people and unexpected emergencies that goes along with this profession.

Understanding scheduling is necessary, whether or not you have in-house security or contract security. Either way, you will want to understand all the parameters for budgeting, training, retention, hours to staff, requirements, vacations, holidays, medical leave, and even union contracts that might affect the scheduling. You will also need to determine factors like patrolling, offering escort services, how many officers a specific task might need, whether inspections are needed, physical demands, the number of entrances and exits that will be controlled, and special assignments.

There are so many choices of scheduling, knowing how many hours and types of shifts you want, will help you determine what resource or programs you will use. There are many computer programs, books, websites, and other resources designed to assist you. Preparing a schedule through the use of a computer-generated software system, such as Excel, is suggested for recording schedules, holidays, sick days, and vacations. Even with this, have an emergency back up plan.

Depending on whether you use your security force on a 24/7 basis or 7 a.m. to 7 p.m., Monday through Friday, you will want to have enough staff to cover such things as overtime, overlapping shifts, training time, flexible scheduling, and supervision. Some shifts are rotating, where officers work in regular patterns of days on and days off. Sometimes the shifts rotate and other times they do not. Whether you utilize 8-hour shifts or 12-hour shifts, both can easily be scheduled to rotate days off and/or to rotate shifts. The use of 10-hour shifts is appealing because it can provide 3 days off each week, but since 24 cannot be divided evenly by 10, excessive shift overlap is required to fit three 10-hour shifts into a 24-hour day. If your officer coverage needs are less for a few hours a day, a combination of 10-hour shifts and 8- or 12-hour shifts can be used to adjust staffing levels to fit your needs. Another approach to a 4 day, 40-hour week uses 2–12-hour and 2–8-hour shifts a week.

Saving resources, such as worker's compensation, vacation, health insurance, and other "per employee" expenses, would entail considering more part-time shifts than full time. There are negative sides to this such as retention, officer job satisfaction, etc. Careful examination of the positive and negative sides of each option of scheduling will be invaluable.

Consider making rules such as not allowing an officer to work longer than a designated period of time or ensuring that the same officer works a particular shift, or making rotating shifts the norm. The advantage in this is the officer does not get complacent or too familiar with the company employees.

By doing periodic evaluations of your security force and reviewing the effectiveness, you will be able to determine which scheduling options are best suited for your company.

Know your Security Staff

Are you approachable, a good role model, mentor, and a good listener? You need these skills and many others when you are responsible for picking someone for a specific position and then retaining them. Mentoring and coaching are key elements for a supervisor. Long after you place an officer, you will want to continue developing, training, and coaching them. By maintaining a relationship with them and retaining information in their personnel file, you can reassess their training and skills so that you have an understanding of what responsibilities and challenges they may be ready to take on if an opportunity rises.

Being a good supervisor requires you to have interpersonal skills such as interviewing, coaching, training, performance evaluating, giving corrective action, and knowing when they need motivation or ready for a promotion. By knowing what motivates the individual, you will be better able to retain them. Often times a day of training might add a huge amount of skill and self-confidence. Be willing to invest in your staff by being a leader and a good role model.

The better understanding you have of your officer's skills and abilities, the easier your job will be. Besides listening, you will want to use observation as a method to evaluate the level of skill they have. Some people look great on paper, but have no communication skills. If the position they will be responsible for means dealing with clients, this will not be a good fit. Knowing the level of communication skills, computer skills, stress handling skills, and physical capabilities, will assist you in determining what job they are best suited for.

Continue Employee Development

Once you have that person in place, continue investing in them by allowing them to develop. This can be done by encouraging them to take classes, whether online, in your office, through professional security organizations or secondary education schools. After completing some additional training, rewarding them with something as minor as a certificate acknowledging their achievement can go a long way. Learning something new may give that officer added confidence and more job security.

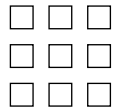
Cross-training your employees can be helpful to your company and provide additional benefits for confidence in your employees.

Personnel Deployment

Quiz

1. The right fit for a position is one of the most critical decisions you will make as a Security Manager?
2. Rarely will you have to consider specific skill sets of the individuals?
3. Paper and pencil tests are a method of determining character?
4. Fully understanding the job description will assist you in hiring the right person?
5. Excel is a great tool in scheduling?
6. Hiring part time officers rather than full time, will help you in retention of your staff?
7. By doing periodic evaluations of your security staff, you will be better able to determine scheduling options?
8. Listening will be one of your most valuable skills?
9. Making an investment in your staff such as providing added training, will pay off by giving them more self-confidence and more professionalism?
10. Maintaining a relationship with your staff will help make you a better manager because it will keep the lines of communication open?

This page intentionally left blank



2 Dealing with Difficult Employees

Ivan E. Pollock

As a supervisor, you will be dealing with many different people, each one having their own unique personality. Most people, however, fit into a grouping of five different types. It is important that you determine which category applies to each individual employee in order to know the basics of how to deal with that particular person.

Determining Personality Types

1. Political: These people are generally more aggressive and demanding; they always look out for themselves and can be very intimidating. To motivate political people, give them some authority and control where possible but make it clear that you are the person in charge. You should be very direct; tell them the end results that are expected and give them a completion date.
2. Aesthetic: These people are very creative and this creativity will always show up in some aspect of their work. To motivate these people, give them the freedom to be creative where possible. For set jobs or procedures, explain why specific methods must be used. Tell them what the standard is; then ask them how we can attain it. They will perhaps require time to do this; as the supervisor you will have to determine if the time required is feasible.
3. Social: These people interact a lot with others, they are motivated, and are generally productive. These people often speak without thinking. To motivate them, set time frames in which to complete tasks. Ensure you praise them for work that is well done. In dealing with these people, it is important to ensure they have enough to do. Lack of sufficient work to fill time will result in this employee disturbing other employees from doing their jobs.
4. Economic: These people are analytical by nature. They are very detailed, are good planners, and usually do things "by the book." These people are motivated to a great extent by information. Let them know that they are right but at the same time watch that they do not spend too much time doing a simple task. In dealing with these people, you may have to tell why a job is to be done in a specific way.
5. Theoretical: These people are highly technically skilled people. They often know more than the supervisor about the job specifics or the mechanics of the job.
   To motivate these people, communicate deadlines for when a job is to be done. In dealing with these people you could use the word "hypothetically"; they will usually think it out and come back with what you want, but believing it is their idea.

Now that the five personality types have been identified, you would think it would be very easy to put each of your direct reports into one of these categories and use the guidelines

I have given for dealing with them. In most cases this will work. In each of these personality types, however, there is the "difficult" employee.

Each of the five personality types can be considered difficult for a unique reason. They can be argumentative, unhappy, angry, talkative, or arrogant. Some may be loners or nontalkers while others may complain constantly or be very indecisive.

The following pages identify various traits of employees that make them difficult. These people can cause major problems in your department regardless of the type of business you are involved in. They must be dealt with effectively or morale in the department will most certainly go down.

The Indecisive Employee

The indecisive employee is similar to the talkative one and can most certainly take up a lot of your time. These indecisive individuals generally do not trust their own judgement and are often afraid of making the wrong decision.

Some of these approaches should work:

1. Be patient; if you try to rush them, matters will become worse. Suggest that they refer to your company procedures and instruction manual. It is better to point out where to find the answer than to just give it to them. Do, however, follow up to ensure that they found the answer.
2. Try to create a relaxing environment; if you show understanding and stay calm, you will make them feel more confident and able to make a decision.
3. Try to set limits; if you can find out ahead of time what they need, you can direct them at that time to research their own answer and therefore make a decision.

The Angry Employee

The angry employee delivers this emotion with two basic messages: one is based on fact and the other based on his/her personal feelings. The supervisor must distinguish between the two and get past the feelings to deal with the facts. Avoid saying things like "do not be angry" or "calm down, there is no reason to be upset." Phrases such as these will only make the person angrier.

Try some of these techniques to calm the person.

1. Keep your own emotions in check and concentrate on the facts being stated and not the words themselves. Try to see past the anger. Very often, the person's anger and frustration have nothing to do with the problem he is having with your company. It may have been brought on by unrelated problems such as an argument with a spouse, or a personal family problem. You can deal with the employee more effectively if you know that there are other contributing factors.
2. Try not to be defensive or you will feel that the anger is being directed at you. This is rarely the case. Try to be sympathetic even though you may find the person's problem is minor or insignificant. Listen carefully, tell him/her that you understand he/she is frustrated and assure him that you will try to help him resolve the problem. Do not, however, agree with criticism of your company. If you agree, you will be telling him/her that he/she is right in being angry, or he/she will lose his respect for you knowing that you, the supervisor, do not support your own company.
3. Stress what you can do to help resolve the problem, not what you cannot do. Negotiate a solution that is acceptable to you and the employee. It is important that you do not promise to do something that you cannot do. It is also important that you do act to bring about the solution to which you agreed.

The Argumentative Employee

The argumentative employee is someone who thrives on arguments. They are always aggressive people who will not agree with anything you say, or at the very least will question what you say.

Do not allow yourself to deal with this person on the same level of behavior by disagreeing and arguing back. This is very possibly the only reaction they were trying to get.

Try these approaches.

1. It is important that you speak softly. Loud speaking will result in a louder response and very quickly result in a shouting match.
2. Due to their aggressive nature, these employees like to feel that they are in control of the situation. If they feel they are losing that control they will become more argumentative. Try asking that employee for his/her opinion. Often they will have a good idea which they just do not know how to present in any other manner. If there is a positive point that you agree on, be sure to say so.
3. It is very easy with this type of person to become irritated and angry yourself. If you feel this is happening, ask the person to leave your office and return in 5 min. If the location does not allow for that, excuse yourself from the conversation and take time to regain your composure.

The NonTalker

The nontalker is a particularly difficult employee to deal with because of the fact that he/she is so quiet. He/she may not be sure of himself/herself or may be doing a great job operationally but just has a hard time expressing himself/herself. It is important that this employee first be identified to ensure that he/she does in fact do a good job and to ensure that you do not lose a good employee because he/she feels unnoticed or unimportant.

With the nontalker you must be patient and make him/her feel at ease. Ask questions that require short answers as opposed to long elaborate ones. The employee should feel quite comfortable with this. Watch for body language transmitted by this employee. He/she may be agreeing verbally with what you are saying, but his/her facial expression is saying something else. Make a point of speaking with this individual at every encounter even if it is simply to say "Good Morning" or "How was your weekend?" These are nonthreatening questions/comments and you should get an open response. It may take time to get this employee to speak freely but do not give up on him/her. They are usually a real asset to your company.

The Habitual Complainer

The habitual complainer does not like anybody or anything. This type of person must be considered dangerous to your department as a whole as he/she will bring down morale on his/her shift or team and it can eventually spread through the whole department.

The following techniques may work.

1. If this habitual complainer speaks to you about a concern, try to be open and let him/her talk. If the complaint is in fact legitimate, take the appropriate action necessary to correct the cause of it.
2. If you hear of constant complaining in the department, you should speak with the person originating the complaint and make it clear to them that their complaints must be directed to you, the supervisor. At the same time, you should let the employees on the receiving end of the complaints know that they should redirect the complaints and not listen to them.
3. As a supervisor, it is up to you to distinguish between legitimate and frivolous complaints because it becomes easy to assume, in this employee's case, that none of his/her complaints are legitimate.

Conclusion

Dealing with nice employees is easy. Difficult people, on the other hand, can be a challenge. Through proper handling of these challenging people, you will gain loyal employees for your department and therefore your company. You will, at the same time, gain a very rewarding personal satisfaction.

Keep in mind that you will not always be successful in dealing with difficult employees. You may have to ask for the expertise of your personnel department or recommend to the employee that he/she seek the council of the company employee assistance program, if available.

As I have mentioned, each individual personality is unique even though we all fit somewhere in the five personality types. In dealing with all employees, I would put it all into one line by saying: "Be participatory when you can, be autocratic when you have to be."

You have read many articles dealing with difficult people and the advice given was about the same, just stated in slightly different ways. It is up to you, the supervisor, to use the advice or not.

Dealing with Difficult Employees

Quiz

1. These people are generally more _____ and demanding.
2. The _____ employee is similar to the talkative one.
3. The _____ employee is someone who thrives on arguments.
4. The _____ is a particularly difficult employee to deal with.
5. Dealing with _____ employees is easy.
6. Political people are generally aggressive and demanding. ☐ T ☐ F
7. Economic people generally do things their own way. ☐ T ☐ F
8. Difficult employees can severely alter department morale. ☐ T ☐ F
9. You should speak loudly and aggressively to an argumentative employee. ☐ T ☐ F
10. Using the guidelines given, you will always be successful handling difficult employees. ☐ T ☐ F

3 The Supervisor's Role in Handling Complaints and Grievances

Inge Sebyan Black and Christopher A. Hertig

Grievances are concerns, problems, or complaints that employees raise with their employers. One of the responsibilities of a supervisor will be to handle these grievances or as we will refer to them, complaints. Handling complaints is never easy and is always going to be part of a supervisor's job. Properly addressing complaints helps to preserve morale, loyalty, and confidence in the supervisor by the employee. Improperly handling complaints is a major source of workplace discontent.

There are various procedures that each particular employer may have. These vary considerably between private companies, public employers, and unionized workplaces. Whatever procedure is in place must be followed. Failing to do so may come back to haunt the supervisor, manager, and everyone concerned at some future point.

Each particular scenario may have a unique twist to it because when dealing with individuals, it is difficult to predict every possible set of circumstance. There will always be unforeseen dynamics due to the character of individuals. Just when one thinks they have heard every complaint possible, a new one is bound to arise!

Whatever type of procedure is in place; the supervisor will want to do the following:

- Always resolve disputes in a timely manner.
- Provide an agreed to, resolution.
- Involve all necessary staff, that is, human resources, union representatives, etc.
- Be externally defensible if for some reason the decision is subsequently challenged.
- Treat every complaint as serious. They are serious to the person bringing them forward.
- Most importantly, be perceived as being fair.

Procedures for unions are spelled out individually by their particular collective bargaining agreement. In public sector employment there is often an additional layer of bureaucracy added in the form of civil service laws.

Many companies now utilize arbitration agreements. Employees sign this while in new hire orientation and it explains the protocol for handling a complaint. Even without an arbitration agreement, every new employee handbook should set out the employer's procedure to handling complaints or grievances, just as they explain dismissal and disciplinary procedures. Some companies also utilize consultation services, sometimes as an employee help line, which helps sort out the issue to the appropriate resource. They may even set up the case and assist management in formulating an appropriate response.

When supervising employees in any setting there is never one response that fits all situations. The supervisor will want to work closely with their human resource specialists to ensure that they are familiar with the employer's procedures.

When hearing complaints, deal with them immediately rather than letting them become a bigger issue that could lead to resignations. Issues left unresolved tend to fester with the end result being the loss of an employee. Procedures that the employer has should be of assistance to both the supervisor and employee when a complaint surfaces.

Processing the Complaint

1. Ensure a high level of familiarity with employer procedures and follow them correctly.
2. Have meetings privately and allow employee to talk without interruption.
3. Listen carefully and take notes (it may also be desirable to have the employee to write down the complaint).
4. Ask questions until there is a total understanding of the facts. The supervisor hearing the complaint may have to interview and probe for specific facts.
5. Repeat the complaint to ascertain full understanding of it in its entirety.
6. If the complaint relates to the complainant's manager, be sure there is another person who they can go to.
7. As necessary and appropriate, direct the conversation to the following topics.
   - Your limitations and your responsibilities.
   - Your company's commitment to and constraints on confidentiality in handling information.
   - Focus on specific details. As appropriate, ask the individual if it is okay for you to take a few notes.
8. Weigh all information to determine what needs to be addressed. Do not make any decision until possessing all the facts, which might involve interviewing others. It is always better to postpone a decision than to make one that will be regretted or have to reverse at a later date.
9. Ask what the employee wants to see in the way of resolution.
10. Check to see if there is a policy addressing the current complaint or if there were similar cases in the past and how they were handled.
11. If the complainant requests to take no action.
    - Document the discussion.
    - Explore with the individual their reluctance to take the complaint further.
    - Let employee know you are available for further discussion.
    - Contact human resources for additional suggestions in meeting your obligation to address this situation.
12. Invite the individual to return if needed.
13. After discussion with the employee (document it completely):
    - Determine if the situation, incident, or discussion needs a written record.
    - Record as soon as possible.
    - Describe the situation.
      - Be objective.
      - Be precise about time, dates, and locations.
      - If quoting, be as precise as possible.
      - If agreements are reached, state clearly what they are and when they come into effect.
    - Consult with a Human resource specialist if one is available.
14. Advise the employee of the decisions as soon as possible. Also thank the employee for bringing this to the company's attention.
15. Follow through with whatever actions are necessary as soon as possible. Delays may result in additional problems.
16. What to avoid documenting:
    - Interpreting behaviors into motives. Avoid conclusion in your writing. Simply describe the behavior.
    - Making subjective statements and giving judgments.
    - Implying corrective or disciplinary action will occur.

- Sharing the document with other persons who do not have a right to access. Observe confidentiality.

As a supervisor, it is challenging to find the balance between protecting everyone's First Amendment rights (to freedom of speech), and encouraging everyone to always be professionally courteous. This is often a difficult balance to achieve. The best prevention is education, training, and encouraging people to talk to a supervisor if they have a concern.

It is imperative that supervisors be trained on harassment prevention. We can take California as an example. They put a law in place in 2005, codified as Government Code Section 12950.1, requiring all employers with 50 or more employees, to train all supervisors on harassment prevention with 2 hours of training every 2 years. It states that the training be interactive and must cover all state and federal laws prohibiting harassment. Although their guidelines on the subject of training are somewhat vague, this can be seen as an example of possible future state or provincial requirements. The California code further suggests that supervisors can be held accountable and personally liable if they ignore illegal conduct when they have the authority to stop it.

Complaints or grievances should be handled confidentially, seriously, sensitively, impartially, and sympathetically. Any breach of confidence can damage a person's reputation. This covers such things as records and the manner in which they are stored and used. All parties, both the complainant and the person complained about, have a responsibility to maintain confidentiality. Employers without them should develop specific procedures for sensitive matters such as discrimination, bullying, and harassment.

Consider having a policy specifically dealing with "whistle blowing" so that workers are encouraged to come forward with complaints. Various laws protect whistle blowers such as the American Sarbanes-Oxley law, public health regulations, safety regulations, etc. A generic policy for handling whistle blowers is a necessity; even if the particular situation is not covered statutorily at present. Organizations should always be prepared to uncover evidence of wrongdoing. The security function by definition plays a leading role in this.

Complaints sent up the organizational chain should be handled by someone who is respected, and who is accepted, as impartial. In some organizations there are boards to handle complaints.

Complaints should not be seen as a nuisance because they provide a valuable opportunity to resolve potentially damaging conflicts and maintain a productive workforce. Following procedures give employees an opportunity to redress injustice. They provide a means to ensure or restore good working relationships. So long as the policy is followed, all parties know that the process by which complaints are handled is fair. Supervisors should steadfastly resist the temptation to bypass procedures.

Prevention

To prevent and reduce the amount and severity of complaints there are some steps that organizations can take. Supervisors should know and follow these procedures as they exist. In the absence of complaint prevention/resolution processes; supervisors are advocates for establishing them. A few simple prevention steps that companies can take are as follows:

1. Have clear policies and procedures in place for complaints.
2. Know the policies. As a supervisor, one should be able to articulate the policy and to understand how it is implemented and enforced. Supervisors must also know who is authorized to handle and investigate specific complaints.
3. Know the laws, local, state/provincial, and federal. Understand the legal definition of such topics as harassment.
4. Train all management staff that may reasonably be expected to deal with complaints.
5. Be prepared to take steps to remedy the employee complaint. Any offensive conduct must be eliminated at any cost, up to and including termination of the employee perpetrating any harassment.
6. Prevent any retaliation against those who complain or those who support a complainant.

Conclusion

Handling complaints and grievances is a major part of a supervisor's job; one that is very important. Supervisors who are adept at resolving the issues that concern their subordinates form a lasting bond with and earn the respect of those subordinates.

Those that do not become isolated from the people they supervise and often witness an increased amount of dissatisfaction, absenteeism, and turnover. No one wins in that situation.

To address complaints better, the "COMPLAINTS" acronym has been created:

C—Consider complainant's perspective.
O—Openness. Maintain openness so that subordinates feel comfortable in bringing you their concerns.
M—Maintain the chain of command. Make sure that the complainant saw their immediate supervisor first. While there are exceptions to this; they should be few and far between. Organizations that lose their chain of command become dysfunctional. All sorts of negative behavior follow.
P—Policy. Consult it and follow it.
L—Listen to the complainant. Something is bothering them. And they may be displaying a significant amount of moral outrage in bringing the complaint to you. Observe them to see all messages being sent.
A—Ask questions. Get clarification on the scope and nature of the issue.
I—Investigate the complaint and report it. Document the complaint.
N—Never belittle the complainant. The complaint is important to them. And they do not share your database; they may not see all the aspects of something that you do.
T—Take appropriate and decisive action. Do not vacillate.
S—Subordinates. Very important people! Keep them informed regarding the status of the complaint.

Practical Exercise: think back to the last complaint that you received. Write the COMPLAINTS acronym and evaluate how you addressed the complaint via the acronym.

The Supervisor's Role in Handling Complaints and Grievances

Quiz

1. You should handle a complaint _____ (when).
2. Confidentiality is critical when handling complaints. ☐ T ☐ F
3. Supervisors should receive regular training on proper procedures on complaints. ☐ T ☐ F
4. Employees should be told about their company's procedures on complaints and grievances when hired. ☐ T ☐ F
5. Human resources can assist supervisors in dealing with complaints. ☐ T ☐ F
6. Never ask the complainant what they want to see as a resolution. ☐ T ☐ F
7. The person taking the complaint should always remain objective. ☐ T ☐ F
8. Interpreting a motive from a behavior is a recommended supervisory practice. ☐ T ☐ F
9. Documenting everything is an important part of the complaint handling process. ☐ T ☐ F
10. In some states such as California, supervisors are mandated to receive harassment-prevention training. ☐ T ☐ F

4 Unethical Acts by Security Officers

Neal E. Trautman

Security administrators must be held accountable for having the courage to "do the right thing" when it comes to instilling integrity and preventing unethical acts by security officers.

The security field is a very demanding profession. While many aspects need improvement, no need is more important than preventing officers from giving in to anger, lust, or greed.

The Problem

Anger, lust, and greed devastate good people and destroy great organizations. Many victims suffer; the family or accused officers are humiliated, fellow officers are ridiculed, and individuals and companies may be devastated financially.

Some people assert it is unrealistic to believe that security officers will abide by high ethical standards while others feel that high ideals and integrity are worthy objectives, yet remain impractical in real life. This is not true.

Leadership, Courage, and Preventing Corruption

Most security companies or departments have never provided any form of ethics training. The reason for this is that most administrators must still be educated about the need for this kind of training while others would rather not face the issues of ethics or corruption at all.

Transforming ethics from the backseat to a compelling high priority is difficult. The two essential ingredients required are courage and a better way of ethics training.

Courage usually requires putting your own fears aside to get the job done. As a term, courage is very subjective. Most dictionaries define it with words implying the ability to meet danger or difficulty with unwavering bravery. We are less familiar with another form of courage: the type of courage required for a supervisor or administrator to actively prevent corruption. It is my opinion that chief administrators face more ethical challenges than cops working the street.

Historically, most administrators have failed miserably when it comes to preventing corruption. Few have ever done more than talk about supporting ethics and professionalism. Corrupt security officers are disciplined or fired and administrators seldom do more.

It takes a lot of courage for the person at the top to do the right thing when corruption strikes. Many administrators do little more than what is "politically safe" for themselves, not what is best for their company. The security profession suffers and good security officers gradually experience a loss of self-respect and loyalty.

Leadership is the foundation for preventing unethical acts. Regardless of rank, a leader's actions serve to guide security officers facing ethical dilemmas. Poor supervision generates bad attitudes, and bad attitudes promote unethical acts. Finally, corruption destroys lives.

Why Unethical Acts Occur in the Security Profession

1. The security profession, like most professions, has a history of corruption.
2. Most security officers have never received ethical decision-making training.
3. Some security officers experience temporary selfishness when faced with temptation.
4. Many security officers do not have strong, ethical role models.
5. Many officers are afraid of paying the price for "doing the right thing" as a result of peer pressure.
6. Security companies neglect to provide assistance for stress.
7. The hiring process is inadequate.
8. Internal training is usually inadequate.
9. Very few security companies have a process that prevents unethical acts from occurring.
10. Administrators create a working environment that promotes distrust and resentment instead of loyalty and respect.
11. The security profession has a reactive, not a pre-active view toward unethical acts.
12. The security profession's code of ethics is not meaningful enough.
13. Security companies lack procedures to identify and deal with officers who exhibit tendencies consistent with unethical behavior.

Leadership Commitment for Change

The first step in preventing corruption is to attain leadership commitment for change. Administrators must show that they believe in the pursuit of ethics and the foundation for demonstrating such commitment is a mission statement. Make ethics a vital part of the current mission statement or, if there is no mission statement, write one. Although developing a mission statement is essential, how it is written is just as important. Do not develop it alone; rather, get the entire company involved; ownership will result.

All aspects of the company should be guided by the mission statement which has a clear ethical direction. Goals are then developed to guide all efforts toward achieving the mission, and objectives are written to assist in reaching each goal. Positive leadership will fuel self-esteem and remove obstacles to attaining these goals.

Initial commitment for preventing corruption can be demonstrated by:

- Assisting in the development of the ethical aspects of a mission statement, goals, and objectives
- Participating in the organization's first ethics in-service training
- Being an ethical model
- Ensuring that all employees are treated with respect and fairness

The path to becoming a truly ethical organization begins with the administration's commitment. Making the commitment may be more difficult than it appears. Most managers and supervisors feel that they have already made such a commitment. After all, they are dedicated, sincere, and loyal to the highest ideals of the security profession.

It is traditional management that can generate difficulties in carrying out the commitment, where old principles of leadership must often be transformed. Without knowledgeable and respectful supervision, all efforts to prevent corruption will be perceived as meaningless.

Training Security Officers to Make Ethics-Related Decisions

Under pressure, people react the way they have been trained. Security organizations have never prepared officers to make difficult ethical decisions. They lack the skills and abilities to face ethical dilemmas because no one has provided them.

There are four primary reasons why good security officers do unethical things:

1. They lie to themselves with excuses
2. Momentary selfishness

3. Bad ethics-related decision making
4. They are afraid of peer pressure reaction for doing the right thing

Ethics decision-making training for officers is not difficult or time consuming. It can be taught to most officers in 30 min. A summary follows.

What "Doing the Right Thing" Requires

It does not matter how difficult or stressful the situation is, in order for your decision to be right, it must support ethical principles. You do this by:

- First setting aside illegal choices
- Then "doing the right thing"

"Doing the Right Thing" Requires Three Things

- Wanting to be ethical
- Acting on your good intentions
- Being able to think rationally

Rational Thinking for Ethical Decisions

There are four steps to take when thinking about an ethical decision:

- Clearly understand the issues
- Evaluate the facts
- Make the decision
- Follow through

Making the Ethical Decision

When facing an ethical dilemma, run a series of tests through your mind. This will be invaluable in decreasing the emotion and temptation of the moment. Rather, objective, rational thinking will take its place. The tests can be used during a 5-sec or 5-week period. Tests for facing ethical dilemmas include:

- How will it make me feel about myself in 20 years?
- What would I decide if I were being videotaped?
- Am I following the golden rule?
- What would I do if my loved ones were standing beside me?
- Is it legal?

Ethical Training Scenaros

The security profession should do with corruption prevention training what has been done with police firearms training. Realistic, stressful, interactive video training must be developed.

Ethics dilemma scenarios can be developed relatively inexpensively without expensive videotaping. Trainers simply write ethical dilemmas, and officers role play the circumstances which have been presented to them via cassette tape recordings. Realism can be enhanced through sound effects, tape recordings, and exercising. Exercising creates many of the physiological reactions an officer experiences during a stressful, ethical crisis.

The Corruption Prevention Process

The security profession has always dealt with corruption by merely investigating charges of misconduct. If warranted, the concerned officer is typically reprimanded, suspended, fired, or in extreme cases, arrested.

Developing and carrying out a highly effective and efficient, all-encompassing corruption prevention process is absolutely essential. Failure to have such a process is one of the primary reasons misconduct continues. To be effective, the process must govern everything that may influence ethical conduct.

Conclusions

Ethics is the security profession's greatest training and leadership need. Our need has resulted, for the most part, from the failure of administrators to actively address corruption and ethics training.

Corruption cannot be eliminated. It can, however, be substantially prevented within any security organization. This can be accomplished, in part, by training security officers how to make ethical decisions. Afterwards, realistic dilemma training will allow them to practice making decisions during ethical dilemmas. This will cement the decision-making process into their long-term memory, and they will react the way they have been trained.

Lastly, security companies must stop viewing corruption as something we react to. Instead, it should be considered preventable. Administrators must maintain a process that prevents unethical acts.

Unethical Acts by Security Officers

Quiz

1. Anger, lust, and greed _____ good people.
2. Historically, most _____ have failed miserably when it comes to preventing corruption.
3. Security companies lack procedures to identify and deal with officers who exhibit _____ consistent with unethical behavior.
4. When facing an ethical _____ dilemma run a series of tests through your mind.
5. The security professional has always dealt with corruption by merely _____ charges of misconduct.
6. Most security companies or departments have been provided with a form of ethics training. ☐ T ☐ F
7. The first step in preventing corruption is to attain leadership commitment for change. ☐ T ☐ F
8. Ethics is the security profession's greatest training and leadership need. ☐ T ☐ F
9. Under pressure, people do not react the way they have been trained. ☐ T ☐ F
10. Corruption can be eliminated. ☐ T ☐ F

APPENDIX A: A Model for Ethical Decision Making

Christopher A. Hertig

Ethics

Ethics is the study of morals within a profession. It is based upon moral theory and applied to situations that present themselves every day. Aside from the theoretical aspects of the study of

ethics, ethics is the practice of moral, professional behavior. Applied ethics is what we need to inculcate within the security industry if it is ever to become a true profession. Applied ethics is what security practitioners must master in order to avoid all the problems of making the wrong choices.

Security supervisors need to do all they can to develop ethical behavior among their subordinates. This will require that various, mutually supporting approaches to this be taken. It will mean a "war on several fronts." A few of the approaches that can be taken are:

1. Having a visible code of ethics displayed
2. Modeling ethical behavior—leading by example
3. Having officers sign a code of ethics or oath or office when being hired—and at regular (annual) intervals
4. Maintaining a supervisory relationship where subordinates ask for clarification from supervisors on ethics questions
5. Proper training in how to perform the job so that the probability of unprofessional behavior being manifested is minimized
6. Training in ethics that enables officers or investigators to make ethical decisions

The following acronym—PORT—is an easily employed ethical decision-making model. It provides a framework for how to make an ethical choice. As such it can, and should, be utilized for instructing subordinates in ethical decision making.

The first component of the acronym is **PROBLEM**. Defining the problem at hand is the first step in solving it. Writing a problem statement is the first step. As ethical dilemmas are conflicts or "hard choices" a problem statement can be composed in a simple manner by stating "There is a conflict between …"

The next step is **OPTIONS**. These are courses of action that can be taken by the problem solver. Many instances of poor decision making occur when all of the available options are not seen by the person "owning" the problem. As with "brainstorming," the trick here is to list all of the imaginable options. Those that are ridiculous should also be listed. By putting all of the conceivable options out for assessment; the chances of picking the best one are improved.

Those options that cannot be seen cannot be employed.

Note that in many cases the best option is a hybrid between several that are listed. Two options are combined into a third option. This is another reason for listing as many courses of action as possible.

In all ethical decisions an option must be chosen and implemented.

The third step is **RESPONSIBILITIES**. Persons making ethical choices have responsibilities to different entities. A protection officer being asked to ignore and cover up the brutal behavior of a coworker toward a detained person has responsibilities to the following entities:

him/herself	his/her family
the employer	the profession
the client (in some cases)	the public
employees	other officers
the law local police	the suspect

The amount of responsibility or obligation owed to each entity can be prioritized. They can be ranked numerically. As part of the decision-making process this should be done.

As with options, as many entities that the officer has responsibility towards should be listed as possible. There will be different entities listed for different situations: victims may be present, contractual relationships may be present, labor unions or media may also be involved. This varies. The important point is to list and prioritize as many entities that are affected by the course of action the officer decides to take as possible.

The final step is **TIME**. The test of time. Very simply this is asking oneself about future feelings:

"How will I feel about myself in 20 years?"
"Will I be proud enough of the decision I made to tell my grandchildren about it?"

Instructors can simply present some realistic ethical dilemmas and have those in the class resolve them using the PORT acronym. This gives the students/subordinates/learners something useful that can be transferred onto the job.

5 Interpersonal Communications

Guy A. Rossi

Interpersonal communications is a fundamental skill for anyone responsible for the establishment and maintenance of a stable, relatively predictable environment. This is especially true for those entrusted with the development and implementation of emergency management plans. During emergencies everyone on the emergency response team must have the capability to communicate effectively with others. Good interpersonal communications foster two-way interaction between individuals and groups. Conversely, poor communications only lead to mixed messages, distrust, and conflict. As an emergency management professional working on a critical incident the message delivered may lead to a positive outcome or a negative outcome. A negative outcome in emergency management applications could result in body count and/or massive numbers of people arriving at local area hospitals. In fact, ineffective communications could be perceived as negligence due to inadequate command and control during a critical incident. Such a breakdown could result in extensive casualties, property damage, negative publicity for the agencies involved, and major lawsuits!

When the emergency management team members need to communicate with the general public, interaction between emergency management personnel and citizens may be categorized into the following basic areas:

1. Information gathering or disseminating
2. Situational leadership and supervision
3. Conflict management

Information Gathering and Disseminating

In order to gain the attention of someone to listen, interact, or disseminate information you must first persuade them to give you their precious time and attention. In essence, you have 30 sec or less to turn the listener(s) on or off. The following are suggestions that will assist you in maintaining the attention of the listener or audience:

1. Sell your position. You must first be willing to share your honest perspective on the situation that is being discussed. A good communicator selects his words and position with forethought. React ing solely on emotion or seeming to be holding back vital information is a sure formula for disaster. Share a need you have with the listener that will result in a favorable outcome. Asking the witnesses at a fire scene if they are aware of any people trapped in the building is a great, and necessary, ice breaker!
2. Adults are only interested in assisting emergency management personnel with answers to questions that are needed to resolve real issues. If the adult listener feels that the speaker is engaging in dialogue that is disguising the real issues they may turn them off.

3. Simplify your interpersonal communications. Adults can read through information being communicated faster than the words can be said. Keeping the message simple assures that the listener's perception of what you are discussing is the same as yours.
4. Use terms and words that the listener is familiar with. Believing that the listener will be able to decode a term or a concept that they may not be familiar with will become distracting as the listener attempts to figure it out.
5. Use words that are action-oriented, visually stimulating, and energized that tend to be motivating the listener to cooperate. Remember, emergency personnel arriving at the scene of an incident are often strangers in that environment. They must build trust with the people they intend to communicate with.

Situational Leadership and Supervision

Emergency management requires leaders who know how to lead during the most stressful situations. The key to leadership in a management role is the ability to influence people. Several studies of subordinates regarding their managers and leaders suggested that successful leaders demonstrate the following traits:

- Honesty
- Competency
- Foreseeability
- Ability to inspire others
- Credibility

When at their best, leaders do the following:

- Challenge the process
- Inspire a shared vision
- Enable others to act
- Model the way
- Encourage the heart—celebrate success and recognize accomplishments!

There are three basic management styles that leaders use. These are:

- Autocratic—rules by fear or a compelling pressure to get things done.
- Democratic—flexible, participative, shares responsibility.
- Laissez-faire—a country-club manager, friend to all. Translated from French, meaning, "Let things alone."

Autocratic Style of Management

There is one significant concept termed "situational leadership." In theory, a supervisor must from time to time be able to demonstrate all of the above leadership styles, depending on the situation that they confront. For example, during a high stress situation supervisors are required to direct priorities. They will likely appear inflexible because of the scenario unfolding before them. This style most parallels military thinking through a chain of command. Although necessary at times, this style is not one that will endear subordinates when used exclusively and the situation no longer dictates a quick decision. Adults will follow this style of leadership when necessary, however they will rebel against it when the situation no longer dictates its use.

The autocratic style may also be used for the subordinate who consistently rebukes the supervisor's authority. A word of caution however, it is critical that a supervisor has the ability to follow up on his commands through discipline, pay, or employment. Without authority, the supervisor's command becomes unenforceable.

Democratic Style

Being flexible as a supervisor and objectively listening to your subordinates is one of the highest forms of respect that may be demonstrated by a supervisor. We have all heard the saying,

"There's more than one way to skin a cat." Whenever you have a group of people, "stylistic" differences will surface. The autocrat will never condone "stylistic" differences, because his/her way is the only way! The democratic leader on the other hand looks at the end result. If the task performed differently achieves the same goal without added expense or burden, he/she should condone the procedure as a viable alternative. By objectively considering suggestions the subordinate feels they "buy in to" the organization and that he/she participates in the success or failure of the organization. Take a look at your organization's most respected supervisors and you will conclude that this is a common thread of the successful, respected supervisor.

Laissez-Faire Style

This leadership style works best in one of two situations:

1. The subordinate is doing an excellent job requiring little supervision. Note: In this scenario the Laissez-faire style reinforces confidence in the subordinate.
2. The subordinate refuses to follow suggested operating procedures, ignoring a supervisor's warnings.

We have all heard of the saying, "If it's not broke, don't fix it." Laissez-fare leadership is a double-edged sword. Either the supervisor recognizes that the subordinate needs little or no supervision or the subordinate fails to respond to a supervisor's suggestion and has taken his own course of action. The bottom line is that the supervisor may delegate tasks, but he cannot delegate responsibility. The supervisor still has to answer to his superiors. Supervisors usually opt for this style of leadership when an employee has been counseled about deficiencies in the past, and continues to disregard the supervisor's suggestions. This style tends to work when the supervisor has advised the subordinate that if he continues in the same manner he will face the consequences without his support. When employing this method as a management tool it is important that the supervisor's superiors are made aware of the management style by choice. The latter is significant so that the superiors are aware that the supervisor has intentionally chosen this style rather than by default.

Remember, leadership is not just about leaders, it is about followers as well. It is a reciprocal process, requiring that it occur between people. Lastly, successful leadership depends far more on the follower's perception rather than the leader's abilities. Remember, perception is reality! If the subordinate perceives that the supervisor is officious, dishonest, or incompetent, supervision will be a difficult task. During an emergency, that interpersonal communications difficulty could be the difference between life and death.

Team Members Who Fail: Counseling Suggestions

It is important that as an emergency management supervisor you build and maintain credibility with your subordinates. A good leader asks himself/herself first, "What have I done wrong to cause the subordinate's unacceptable behavior?" If the leader can objectively answer this question with, "Nothing," then a counseling session is in order. The following five suggestions may serve to foster a more positive image:

1. Clarify your values with the subordinates.
2. Identify what your subordinates want and need.
3. Build a consensus and work towards the same goal, finding shared values.
4. Communicate shared values with enthusiasm.
5. Lead by example.

Basic Ingredients of Effective Counseling

1. Praise in public, counsel in private.
2. Be an active listener.
3. Look at the problem from your subordinate's point of view.
4. Establish a comfortable relationship/atmosphere during the session.

The Counseling Session

1. Have a positive feeling about yourself as a supervisor. A positive self-image is crucial for counseling.
2. Gather all pertinent facts first.
3. Summarize and review important material.
4. Stay calm; do not attempt to counsel while emotionally involved in the issue.
5. Call indirect attention to the subordinate's mistake.
6. Listen with empathy.
7. Provide feedback.
8. Invite the subordinate to respond.
9. Think before you speak.
10. Restate the problem, using the subordinate's words to ensure clarification.
11. Identify the policy or proper procedural response for the subordinate.
12. Set goals and objectives to facilitate remedial training.
13. Effect completeness.
14. Celebrate successes.

What You Should Do and Say

1. Allow the subordinate to determine which of his/her negative behaviors they want to work on first.
2. Help the subordinate to establish counseling related personal goals.
3. Help the subordinate to identify logic and/or performance that is self-defeating.
4. Assist the subordinate to reach self-understanding by examining his/her detrimental behaviors.
5. Help the subordinate to establish a maintenance system for the concerned behaviors by finding alternatives.

What Not To Do

1. Warn or threaten.
2. Order, command, or direct.
3. Moralize or preach.
4. Lecture or give logical arguments

Conflict Management

From time to time emergency management personnel arrive at the scene of a critical incident and find themselves in a hostile environment. One of these phenomenon that has been propelled to the forefront for private emergency management teams is characterized as "going postal" (violence in the workplace). Conflict management becomes a priority in the situation when an employee is being assaulted by a spouse or a recently terminated employee returns to work to seek revenge. To be prepared for such an event, it is essential that the emergency response team be trained in safety skills required to "read" a potential conflict and do everything possible to avoid or mitigate violence.

Response Principals

1. Never rush into anything without first obtaining information about the type of conflict you are walking into. If need be, attempt to watch the dispute surreptitiously prior to entering the location. Avoid attempting to deal with the situation by yourself without a backup. Approach from a concealed position as much as possible. Stay behind cover as much as possible. Always "think knives and guns": be in a position and have a plan for confronting them. Remember to always see the palms of the hands to insure that weapons are not being held. If people secrete weapons on their bodythey are most likely to be in the waist area. They may be hidden elsewhere; observing the person for unnatural gait, etc.

2. Assess the violence potential. Use your training in management of aggressive behavior techniques. Separate, defuse, and mitigate. Make as many arrests or detentions of individuals as needed to regain stability of the environment. Speak to everyone present to ensure objectivity as well as to identify other potential assailants. Attempt to keep everyone in sight until assistance arrives.
3. Stabilize the physical situation in an appropriate manner. Avoid crowding people. Stay away from kitchens, and tool shops. Weapons are usually secreted in private areas that are accessible to the combatants. Always attempt to get the parties to interact in a semipublic area such as a conference room, where weapons are less likely to be available. Attempt to get all parties to sit down and to allow one to speak at a time.
4. Maintain control throughout the situation. Defend yourself at all costs! You do not get paid to get hurt nor can you assist anyone if you are hurt. Disengage until help arrives. As long as you follow a policy of notifying the proper authorities, you have done your job. If you use force and are not authorized to do so, your employer may claim that you abandoned their policy, procedure, and training when a lawsuit is later initiated. When authorization is approved, use "only that force necessary to effect an arrest or detention while trying to protect yourself or others—no more, no less! Make certain that the incident is documented and that the public law enforcement officers are advised of the tactics that you used to control the individuals.
5. Know your exit! Remember your firefighting training here; when you walk into any situation, know your way out. Have a plan so that you may disengage quickly if the need arises.

Reading Danger Cues

Body language is defined as unconscious signals sent from the brain that outwardly reflect a person's emotional state. Since words seldom depict the true message hidden behind words, we must learn to rely on the nonverbal communications as indicators of potential assault. Remember, by law you may protect yourself by meeting force with force in order to disengage for officer safety.

Generally speaking, interpersonal communication skills, not force, are what commonly defuse conflicts. Therefore, enrolling in a course designed to reduce a subject's anxiety by verbalization should be a priority of public and private law enforcement training. A program such as "Management of Aggressive Behaviour" (M.O.A.B.), identifies common tactics that de-escalate situations with verbal interaction as well as indicators to potential assault. As stated in the M.O.A.B. book by Rolland Ouellette, your verbal communications must be *reasonable*, *enforceable*, and *enforced* when necessary, otherwise you will risk loss of credibility and control.

There are many other areas of conflict management training, however they are more directed at psychomotor skills and tactics requiring practice in the presence of a competent instructor. Police and security academies usually offer training in these areas. *Training and proficiency in conflict management must be an ongoing process in your professional development*.

Interpersonal Communications

Quiz

1. Approximately 40% of what is said is conveyed by body expression.

   ☐ T ☐ F

2. How many seconds does a communicator have to turn the listener(s) on or off?
   1. 10 sec
   2. 30 sec
   3. 15 sec
   4. 45 sec

3. There are three basic management styles that a leader may take with his/her subordinates, they are _____, _____ and _____.
4. Successful leaders demonstrate the following traits:
   a) Honesty
   b) Competency
   c) Have a vision
   d) Are inspiring
   e) All of the above
5. Democratic management style most parallels military thinking through a chain of command. ☐ T ☐ F
6. Leadership is not just about the leader, it is about _____ as well.
7. Supervision will be difficult if the subordinate perceives the supervisor is:
   a) Officious
   b) Dishonest
   c) Incompetent
   d) All of the above
8. It is against the law to protect yourself by meeting force with force in order to disengage and establish officer safety. ☐ T ☐ F
9. Poor interpersonal communications can lead to:
   a) Mixed messages
   b) Distrust
   c) Conflict
   d) All of the above
10. Which personality trait may be used for the subordinate who consistently rebukes the supervisor's authority?
    a) Democratic
    b) Autocratic
    c) Laissez-faire
    d) None of the above

UNIT IV

Training and Development

This page intentionally left blank

1

Training: Strategies, Tactics, and Challenges for Protection Managers

Christopher A. Hertig

Defining Training

When we think of training we envision teaching or instruction. We think of lectures, videos, training exercises, "showing a new employee the ropes", and tests. Generally speaking, most of us view training by one of its aspects or components rather than as the total process that it is. We view training in a very limited manner. Sometimes we equate it with classes held on a particular topic. In some other cases, we think of it as learning and practicing a particular skill.

While all of these activities are, indeed, training, they are merely components of the process of training. They are but pieces of the "training pie." Training can be thought of as an intense learning process where an individual is taught a skill or knowledge that enables him/her to perform a job function. It incorporates various teaching and learning methods. It involves significant amounts of practice. In addition, training is always tested or validated in some manner.

By internalizing the definition above, a manager who is charged with some aspect of the training process can better discern the impact of their activities within that process. The common mistake of believing that learning—a change in behavior or attitude—has occurred due to a single learning experience (a class, a meeting, an orientation session, etc.) will be avoided. Most people believe that a single well-intentioned learning episode will have a significant impact on job performance because they want to believe it. The astute trainer/supervisor/manager knows that job performance improvement requires *significant effort*! The effective supervisor will know how to integrate training activities into a comprehensive learning system. By doing this, positive changes in job behavior are far more likely to result.

Supervisors or managers who are in charge of training their subordinates must ensure that the training is continuous. The learning must be reinforced through guided practice such as periodic in-service instruction, recertification, drills or scenarios, individual reading or research, and attending classes on the topic. The more separate, yet integrated, learning episodes, the better the learning.

Benefits of Training

The benefits of training must be examined prior to embarking on an expensive, time-consuming training, and development process! In order to ensure the greatest return on instructional dollars, we must understand both the benefits and the costs. Some of the beneficial effects of training are as follows:

- Increased job efficiency where specific job tasks are performed better and faster, thereby reducing manpower costs

- Better relations between employees and management as the employee understands management perspective more—a crucial element in security operations
- Enhanced professional identity by protection officers, who see positive growth within themselves
- Pride and job satisfaction—this can be extensive, it can "turn someone's career around"
- Increased loyalty to the employer, who has shown an interest in the employees by training them
- Decreased turnover as there are fewer situations that make the officers feel uncomfortable and incompetent—a crucial point for younger personnel who can be easily discouraged by failures
- Fewer mistakes
- Decreased accidents
- Improved discretionary judgment, with better decisions being made by officers or investigators
- Protection from allegations that management is negligent in preparing officers/agents/investigators to perform their jobs

Determining Training Needs

Determining what areas security personnel need training in is key to successful, cost-effective training. Training is wasted if it is used to solve problems that are due to inadequate equipment, inadequate resources, or inappropriate job design! Training cannot, by itself, serve to motivate personnel; nor can it solve other problems related to the development of knowledge, skills, or abilities.

In order to accurately assess training needs, it is first necessary to go through a review of the situation at hand. This will illuminate the problems, causes, and possible approaches to addressing them without plunging into an expensive, time-consuming training endeavor.

Some simple questions to ask in this regard are as follows:

1. What is the job performance problem?
2. Is the problem a result of inadequate skill or knowledge on the part of security personnel?
3. How can the lack of knowledge or skill deficiency be corrected?
4. Has the knowledge/skill deficiency been corrected?
5. Does the problem still exist?

Problem: There is a high rate of turnover by contract security personnel at a client's site. Absenteeism is also a problem. Training is minimal as officers are not there long enough to complete anything other than a 4-hour orientation program. The client is considering changing security service firms.

How should addressing this problem proceed from the standpoint of the supervisor in charge of the account?

Types of Training

Lectures are often used as an instructional technique. They can be effective or ineffective, depending upon the circumstances. Supervisors must always bear in mind that adults do not like to be lectured. They must instead be informed and stimulated.

A few things to remember to keep lectures effective are

1. Lecture to establish a common base of knowledge when this base does not exist. Preinstructional assessments can aid with this.
2. Use visuals as much as possible as most people are visual learners—video clips are good in this regard. These should be short, not more than 10 min.
3. Use lectures to assess the learners, what they know, and how they feel about certain topics. Adults like to discuss their opinions.
4. Keep lectures short and to the point as much as possible. Changing the instructional delivery method at least every 20 min or so will help students maintain attention.

5. Only use lectures to make two or three points at a time; more information causes overload and learners BLANK OUT the learning.
6. Reinforce lectures with active learning such as scenario exercises, discussions, and short tests. This changes the pace and requires application of the material being taught.
7. Organize the lecture using the same format as a letter: an introduction, main body, and closing (which summarizes and reiterates the key points); a simple manner of remembering this is to draw an analogy between other means of communication such as letters and interviews, each of which has three parts:
   - An introduction where the topic to be discussed is first mentioned
   - A main body where the topic is discussed in full
   - A closing where there is some degree of summarization or recapping of main points

A simple way of remembering this in an instructional setting is

"Tell 'em what you're gonna tell em.

Tell 'em.

Tell them what you told 'em."

Demonstration is an essential instructional technique for teaching proficiency areas such as equipment use, interviewing, defensive tactics, firefighting, etc. To demonstrate effectively, the following points should be borne in mind:

- Explain what you are going to do beforehand.
- Make sure everyone can see.
- Make eye contact with everyone during the demonstration.
- Demonstrate the entire task so that visual learners can grasp what is to be done in a single demonstration.
- Use video if at all possible to ensure uniformity and documentation of the process to be demonstrated; video also ensures that the whole class can see the procedure being performed.
- Have the class practice the skill at a slow, easy pace and then refine their proficiency.

Coaching or tutoring is also vital for supervisors as it is the essence of supervision. Coaching or tutoring can be done in a myriad of situations on the job. A few ideas to be borne in mind include the following:

- Select the appropriate learning method (reading assignments, incident review, computer-assisted instruction, research project, etc.) for the learner and what is being taught.
- Do not be afraid to use multiple learning strategies; rather look for the opportunity to do so.
- Always build on prior learning—but do not be frustrated if the trainee does not know what you expect them to know. Do not expect trainees to know as much as the trainer—make no assumptions about prior knowledge.
- Be patient and do not expect everyone to learn at the same rate—or in the same manner.
- Be flexible and change strategies if the one originally chosen does not work.
- When editing reports—a great training opportunity—make sure to:
  (a) Praise in some way the work that has been done. Always accentuate the positive in what has been written. Do not trample upon the ego of the writer.
  (b) Question the writer as to what they are attempting to express.
  (c) Polish the report with suggestions for improvement (Feld, 1993).

Roles of Supervisory Personnel in Training

Orienting new employees—within the security department or other departments—is a function commonly performed by security supervisors. Since 9/11 there has been an expansion of this, which creates opportunities for security departments to teach what is expected (Albrecht, 2006).

Orientation is an important juncture in the employment process, combining the selection, training, and socialization aspects of the relationship. Supervisors should make the most of it by doing the following:

1. Spread out the learning as much as possible—try and have several sessions/learning episodes. While the major block of instruction may best be covered in a single day; avoiding learner overload and building upon the initial session is essential.
2. Instruct in the history and philosophy of the organization. While this is often left out or given minimal treatment, it is essential to develop the ability to make the discretionary judgments. Discretionary judgments are integral to the role of the protection officer. Effective socialization of the employee over the long run is possible, as the officer has the foundation of knowledge to form understanding. An additional benefit may be that the officer becomes a more effective "sales rep" for their organization: a crucial element for security service firms!
3. Keep the sessions dynamic and ever-changing: use a variety of instructional techniques—mix it up.
4. Make the employee feel a personal bond to people within the organization by introducing him/her to people such as mentors, supervisors, and upper-level managers. Note: Sometimes inviting upper-level managers to meet new employees can elevate the visibility of the Security Department.
5. Prepare the new officer for orientation by informing him/her as to time, place, topics, and what to expect in terms of dress, deportment, and activities—reduce the amount of uncomfortable situations the new hire is exposed to at all times.

In many cases supervisors are called upon to teach in-service classes. These can be BRUTAL for both the teacher and the learners! While much of the information concerning overcoming resistance to training is relevant to in-service instruction, the following considerations are essential:

1. Get feedback from the officers as to what they want to learn. Surveys of staff can provide some unique insight and prevent unnecessary effort and expense.
2. Become an expert—do research and make it interesting by informing them of things they do not already know.
3. Use different instructors—outside experts, personnel from other departments, and security officers.
4. Keep the class moving with exercises and different activities. This is especially important after lunch.

On-the-job training (OJT) must be provided or overseen by security supervisors! It must be delivered in a professional manner. OJT can be delivered via a mentoring or Field Training Officer arrangement. This ensures that the "instructor" is teaching in a professional manner and not simply missocializing the learner with bad habits and attitudes. OJT can be effective if it is structured and formalized. OJT will be a waste of time or a euphemism for a lack of a training program without organization and structure.

Perhaps the first important aspect of OJT is commitment. OJT must be a priority! It should be delivered in a structured, organized manner using the following techniques:

1. Explain and demonstrate each job step.
2. Demonstrate each job step while the employee explains the process.
3. Have the employee demonstrate and explain each task.
4. Stop by later and follow up on the learning.
5. Document the training by having a form signed that lists all areas (procedures, equipments, and locations) that have been covered.
6. Preface the learning by preceding the OJT with a classroom session and/or individual learning experience such as watching a video or reading a manual.
7. Follow up the learning by having in-service sessions, drills, etc.

Job aids can be an effective method of reducing training costs while at the same time increasing job task proficiency. Simply put, a job aid is an instruction or direction on how to do something.

It can be a sign on a piece of equipment. It may be a procedural manual. It could be a sign or memo that serves as a reminder. The Crisis Prevention Institute (crisisprevention.com) sells posters that list steps to be taken for dealing with aggressive persons. Safety posters and posters reminding persons of information security procedures are other examples of job aids.

Whatever the form a job aid takes, there are several tips to remember about making them effective:

1. Keep sentences short and to the point.
2. List steps to be followed.
3. Leave space around each sentence so that it is easy to read.
4. Use a plain type style.
5. The job aids should be accessible, convenient, and user friendly in every respect.

A mentoring program is where a senior employee guides and assists a new worker on the job. In days gone by this was simply placing a new officer with a more senior one who "showed them the ropes." Such an informal approach enabled the new employee to absorb all the negative traits of the older worker. Mentoring is different because it is more structured. Mentoring may involve a financial incentive to the mentor and should always involve special training and instruction for the mentor.

A few things to bear in mind concerning mentoring programs are as follows:

1. Select a mentor that the new employee should emulate.
2. Provide the mentor with additional, special training, and education so that they may act as an effective coach.
3. Introduce the new officer to the mentor at an early stage in the employment relationship such as at orientation.
4. Mentors should be easily approachable by trainees.
5. Mentors must be good teachers who enjoy passing along their knowledge.
6. Mentors should be able to give the neophyte employee exposure within the organization.

Evaluating training can be a very complicated matter best left in the hands of specialists who have done graduate work in education or training and development. Test design may not be a simple task! In most circumstances, professional test validation is not within the means of the organization. There are, however, other approaches that can be used to assess training. These should all be considered as appropriate to the situation:

1. Have trainees evaluate the training via a predesigned form or by simply asking them to write an essay on their perceptions regarding the program. This is fairly simple to do and provides one perspective. It must be borne in mind, however, that filling out "Happy Sheets" really only measures trainee's happiness with the program, not learning, retention, or transfer to any significant degree.
2. Utilize an employee questionnaire before and after training that assesses the perceptions of employees regarding security force professionalism. This may provide a metric for the effectiveness of the program on the "public's" perception. In certain settings this is a critical factor.
3. Analyze incident frequency and severity before and after training to determine if training had a positive effect on how the officers handled incidents.
4. Analyze incident handling times to see if the amount of time needed to respond to a problem decreased after training.
5. Utilize off-the-shelf instructional programs which contain testing instruments. This can reduce or eliminate the complex, time-consuming task of designing tests. If the subject matter is generic in nature, off-the-shelf programs are generally much more cost-effective.

Another fairly simple method of evaluating training is through the use of supervisory anecdotes. These are simply observations that supervisors make concerning job performance following a training program or session. Anecdotes are simple to use and must be done anyway to evaluate how the new employee is performing on the job.

A few things to bear in mind about supervisory anecdotes are

1. They must be completely objective and not tarnished by the opinions of other supervisors or preconceived notions of the supervisors making them.
2. Supervisors should have substantial input into training design so that competition, jealousy, and general ill-will do not develop between trainers—who may not be supervisors—and the supervisors on staff.
3. Use written questionnaires to evaluate so that all observations must be articulated clearly. The written questionnaires can evolve over time to collect key data.

Problems in Training

Training is often greeted with unbridled enthusiasm. Many people love to teach and think of training in solely positive terms. Unfortunately, there are numerous problems involved in the design, development, and implementation of training. If these problems are not addressed, training will not be effective, may serve to demoralize personnel, and WILL cause budgetary problems. Perhaps the worst—and unfortunately a very common—dilemma that can befall training is that training JUST DOES NOT HAPPEN. This is both an obvious operational dilemma as well as an ethical lapse on the part of supervisors/managers who have a duty to adequately train their subordinates.

Budget restrictions are perhaps the most common problem in security officer training. Most organizations devote very few resources to training security personnel; some spend nothing at all! There are various approaches to take in addressing this problem:

1. Hire personnel with as much training as possible. This in and of itself does not ensure a properly trained protection force—highly trained persons may not have the exact job skills necessary in a specific application—but it may address the issue to some degree.
2. Attempt to have other departments within the parent or client organizations provide instruction. This can include topics such as customer service, time management, safety, business writing, etc. These topics are certainly of value to security officers and having the officers attend training given by other departments can be a very low-cost option. An additional benefit is the integration of the security department into the larger organization. The security department projects positive exposure to the rest of the organization. Also, the department gets a good feel for what is happening within the parent or client organization.
3. Utilize distance education. Correspondence courses are one approach. Having the security staff complete the Certified Protection Officer (CPO) program not only gives the officers a comprehensive exposure to key security topics, but it culminates in a recognized professional credential. While distance education—where the teacher and learner are distant from each other—is not cost-free, it is very inexpensive as it eliminates paying for overtime, so officers can attend classes. It also bypasses the generally insurmountable hurdle of scheduling a class and getting all officers into the class. This can be an even more important consideration when security officers or loss prevention agents are part-time or geographically dispersed.

   Distance education is often not well understood and even denigrated by some persons. There is a lot more to it than commonly thought. Distance education can take a myriad of forms, from correspondence study to Internet courses to having officers utilize video or audio tapes during quiet times. Online learning communities can be created or joined. Simple e-mails can be used to inform staff members. The astute learning manager understands this and applies the various forms of distance education appropriately. A very simple use of distance education is to have officers read policies and procedures on their own and then answer questions on them. The questions can be developed by the supervisor in completion, essay, or fill-in-the-blank format. Such an approach eliminates costly classroom time spent going over mundane items that the learner has access to on his/her own. It can be incorporated into computerized

instructional formats or used in concert with audio or video tapes. Care should be taken to reinforce and clarify the learning with person-to-person instruction (highlighting at training meetings, reviewing with individual officers on post) so as to ensure comprehension. Utilizing distance education in concert with traditional classroom instruction can offer the best of both worlds. Additionally, it can be used before or after a classroom session as a means of reinforcing learning. An example would be using the CPO program chapters on interviewing or first aid; the student can read these chapters and answer the questions at the back of them before attending a classroom session on either topic. One cannot effectively teach interviewing or first aid from a book, but one can introduce the topic in this manner. Additionally, one can reinforce and expand upon a classroom learning experience via use of a manual.

Online courses have grown in popularity throughout the contract and retail loss prevention sectors in particular. Large security service firms and major retailers have centralized training functions with web-based or CD-ROM programs. Online courses can be very cost-effective and can adjust to the varying learning styles of participants. Dynamic programs are likely to capture the attention of contemporary learners. They may also significantly reduce learning time and expand learning content. These are key factors in any training or educational endeavor. Additionally, the metrics within various programs are quite useful for keeping track of learning progress.

Problem: After suggesting that the security force be enrolled into the CPO program, a supervisor is told by his/her superior that "correspondence study is a bunch of B.S." What arguments could be used to persuade the manager? What facts and research are available to support those arguments?

4. Tuition reimbursement can be used to inspire persons to improve their individual educational/training level. Many organizations have earmarked tuition assistance money; unfortunately, many security departments have not taken advantage of it. While this does not ensure a baseline foundation of knowledge, skill, or ability for the entire security force, it does help to promote professional development. Professional development always pays for itself in one way or another at some point.

Scheduling is a serious impediment to traditional training classes for security departments. In order to get everyone in the class, the session must be scheduled AT LEAST TWICE! This is to compensate for officers on post, officers out sick, officers on vacation, newly hired officers, etc. The reality of security training is that unless ALL officers are trained BEFORE being assigned, classroom instruction cannot be used to train everyone. Unfortunately, few supervisors/managers will fully acknowledge this. The issue is ignored, and uniform, comprehensive training does not occur via traditional classroom instruction.

There are a few approaches to overcoming this seemingly insurmountable dilemma:

1. Distance education, which can be achieved at a learner's own pace and own place, is probably the foremost approach to solving this problem.
2. Give as much training as possible in the preassignment phase of the employment relationship. This eliminates the hassle of attempting to schedule classes later on. It also reduces or eliminates uncomfortable situations that new officers are faced with: a key cause of turnover.
3. Still another approach is to require persons to have certain levels of training prior to being hired or to maintain present levels (first aid, state certifications, weapons certifications). Compensating the officers for doing this may be less expensive and troublesome than attempting to set up "master schedules" for all security force members.

As emphasized earlier, real learning and positive behavioral change does not occur in a single learning episode. People can only learn so much at one time. People only pay attention a fraction of the amount of the time they are in classes. And people must be ready to learn certain things at certain levels of maturity, education, experience, etc. We all learn differently, and we all learn different subjects at different phases of our lives.

Obviously, a comprehensive, continuous learning system is necessary. Reinforcing the learning can be accomplished by

1. Periodic in-service instruction, such as quarterly qualification with firefighting equipment or weapons. This should reiterate and build upon previous knowledge, skill, and ability.
2. Drills or scenarios, where the concepts are applied to actual situations. Scenarios can take many forms. In a session teaching about policy and procedure, a hypothetical problem can be constructed to assess how the trainee applies their learning. "Table-top" exercises can be done in group setting to determine the response to specific loss events. Drills affecting only a portion of the facility or protection operation or full-blown scenarios involving off-site agencies can also be used.

   Problem: Pick a work environment. As a security supervisor within that work environment, what sort of practical scenario exercises could be developed? Making sure that officers are only being tested on what they have previously been taught, what type of exercises could be developed that would not cause operational or safety problems?
3. Job aids in the work environment that serve as reminders of how to perform a certain procedure. These include procedural manuals, signs, and sets of instructions on security equipment. Job aids can go a long way in ensuring that performance levels are maintained. They can also reduce costs for instructional sessions. Using job aids effectively can be a very cost-effective training strategy. Performing a study/audit of those in the work environment can be a good first step in employing this strategy.
4. Reviewing procedures and post orders with officers at their duty stations. Spending a few minutes with officers is an essential part of the supervisory process; integrating training into this time is a good way to structure supervisory visits.
5. Sending officers to classes on work-related topics. These can be at local community colleges, training academies, professional meetings, etc. Local chapters of professional organizations such as ASIS can host annual programs for security officers. In some areas, groups of security directors at hospitals and colleges are already doing this. Note: cooperative training sessions, group enrolments into the CPO program, cooperative purchasing of CDs, videos, etc. by security associations may be THE WAY to make training affordable and accessible!
6. Completion of the safety course offered by the International Association of Healthcare Security & Safety (IAHSS). This approach is used by many hospital security directors who benefit by developing the safety knowledge of their officers. It is an excellent reinforcement and enhancement of previously learned safety material, which serves to expand the capabilities of the protection force. Health care protection administrators who have their officers first complete the IAHSS's basic standard and then the safety program during the next year can expect a significant amount of demonstrable, recognized organizational development to occur. The same may be true for retail or investigative sector managers who use the IFPO Crime and Loss Investigation program in a similar manner. The baseline; the foundation is built with the CPO. After that specialized instruction in investigation is completed.
7. Encouraging officers to attain licenses or certifications to use weapons, equipment, administer first aid, lifesaving, Water Safety Instructor, etc. These activities all help the employee to grow and become more valuable to the organization. They increase the capabilities of the Security Department while at the same time addressing each member's individual learning needs. Note: while not all activities precisely fit the organization's immediate or foreseeable needs, some flexibility is desirable to keep personnel motivated.
8. Membership in professional organizations such as IFPO or subscribing to professional publications such as security or police and security news are other methods of enhancing the continuity of learning. An added benefit to this is that protection officers get a professional identity.

9. Incidental learning by making books, magazines, etc. available to officers is another useful technique. This costs next to nothing, keeps staff abreast of what is going on in the industry and further reinforces the concept of professional identity: officers see that there is a substantial body of knowledge along with an expectation by management that they delve into it.

   Problem: The general manager of a contract security firm wants to see a new culture of professional growth/identity within the organization. At a branch office employing 1,000 officers which is part of a national firm, how could this strategy be utilized? What specific steps could be taken?

10. Overlapping the learning by having class members write descriptions, give class presentations, take notes, and conduct interviews throughout the instructional process. Report writing, for example, cannot be effectively taught in a single session. There must be continuous practice of the writing skills. The same is true of speaking in public (testifying, crowd management, supervision) or interviewing. By having active participation in problem-solving exercises, key skills can be honed and refined. An example would be having an officer testify in class as to his/her report; the primary purpose is to teach testifying skills, the ancillary objective is to reinforce and refine report writing skills. Another example would be having class members conduct interviews and take notes so that interviewing techniques and note-taking methods are taught. Such an exercise could be conducted at some time after a note-taking or interviewing class.

Bureaucratic training can be a major problem in some environments. This occurs when training is done only to satisfy government requirements. The bureaucrat only trains to minimal legal standards. While legal mandates must be complied with, merely adhering to them is not enough. Officers quickly see the halfhearted approach to training and are turned off to "training"! "Going through the motions" is seen as just that. As a result, protection officers are demotivated to learn and may block out future attempts to enhance their job capabilities.

Training should serve to create and improve job task performance. Compliance with legal standards—while a necessity—is best thought of as a positive by-product. Making compliance the primary goal of training is wasted training! The troops are not impressed. Neither are many government inspectors.

Problem: A manager whom the supervisor reports to believes that all the training that is necessary is that which is required by the state or province. He/she does not want any additional funds spent on training. What arguments could be advanced to persuade this individual that increased training is beneficial?

Resistance by learners is a significant problem facing those charged with training. In many cases personnel do not want to be in a particular training session or do not want to learn a new procedure. Some methods of dealing with this include the following:

1. Take care in scheduling the training so as to interfere with the learner's life/schedule as little as possible.
2. Recognize the experience, knowledge, and contributions that each officer can make to the training experience. Adults need to be stroked! A genuine compliment can go a long way toward decreasing resistance to learning.
3. Ask the trainees what they want out of the training. Try to incorporate their needs in the design and implementation of the training as much as possible. Training is not the product of a single individual. There are various people involved including management, publics that are served, and the persons to be trained. Good instructors understand this.
4. Provide incentives. These can be small or large, depending upon the situation at hand. A list and photograph in the company newspaper is one way to reward those who have completed training. Giving out of certificates and plaques is another. Providing meals and refreshments is also a nice gesture. Letting the class go early is also appreciated by the learners.

5. Deal positively with trainees who utter questions meant to challenge the instructor or content of the learning. Sometimes these questions can be reflected back with a "How would you handle that?" Asking the class for their input is another strategy. Sometimes telling the hostile questioner in a classroom setting that the question will be resolved over break—and following through with the promise—is necessary.

"Stuffed Shirts." These are security supervisors who have obtained their positions due to their educational backgrounds. They have a college degree but not enough experience or specific training to be competent. They never went to any type of academy and generally do not understand the realistic applications of firefighting, handcuffing, crowd management, etc. While everyone has weaknesses in their background, it is important to see those weaknesses and work with them in a positive manner. Supervisors are not expected to be experts in everything, but they must be competent at all essential job tasks. They must also be humble and ask for assistance from others. Supervisors should not hesitate to ask one of their subordinates to assist with a training problem. There is no reason why the talents of the security force cannot be harvested! Most security forces are composed of persons with diverse backgrounds (a medic, a firefighter, a soldier, a police officer, a computer specialist, a safety specialist, etc.). Astute supervisors use their talents.

Liability for failure to train may be imposed upon supervisors who have training as part of their responsibilities. Obviously, there is liability exposure to organizations and the individual supervisors who work for those organizations where officers are armed. As "private security" personnel assume more tasks and have greater responsibility to the public, the potential for liability exposure can be expected to grow. Adequate training, practice, and documentation of the training is a necessity in these situations. Perhaps not so obvious is the potential for liability due to personnel who are not adequately instructed in how to use emergency equipment or who are expected to provide emergency services. A simple method of uncovering liability exposure in this area is to ask the following questions:

- What are the duties that personnel under my supervision owe to their employer, clients, visitors, etc.?
- What types of emergencies that protection officers must respond to are reasonably foreseeable?
- What specific functions are they expected to perform during emergencies?
- What types of equipment/weapons can they be expected to use in emergencies?

Training is essential if performance is to be enhanced to any appreciable degree. Unfortunately, the process of training is complex. It is—on its face—cost-prohibitive if not implemented creatively and managed. The following discussion outlines some of the common misperceptions involving the training of protection officers and how these training dilemmas can be avoided or reduced in severity.

The Definitional Dilemma

"The Definitional Dilemma" begins when managers or trainers do not truly understand what training is. They cannot adequately define training and consequently are unable to differentiate training from education or development. Those afflicted with the "Dilemma" throw all three terms around interchangeably, ignorant of the fact that there are distinct differences between them. To avoid this trap, a complete understanding of what "training," "education," and "development" consist of is needed.

Training prepares the employee through the infusion of knowledge or the acquisition of skills or abilities to perform a specific job. Training focuses on the "how to" do a job task. Training involves practice, repetition, and skill development. The training process is designed to develop a specific job skill, such as driving, using a handgun, patrolling specific points, or administering first aid. Training's focus is on task proficiency.

Education broadens his/her perspective by increasing the employee's knowledge base. Education focuses on the "why" a job task or duty is being performed. An employee who is educated may not necessarily be able to drive, shoot, patrol, or care for casualties; instead he/she

will be able to explain the theoretical foundation behind driving. He/she will understand things such as stopping distance, friction, momentum, etc. He/she will be better able to make judgments about what constitutes safe driving. He/she should also be able to learn faster when in new training courses. At the managerial level, he/she will have a better idea on how to write driving policies and develop safe driving programs.

Development creates growth in the individual and the organization through the combining of training, education, and new opportunities. As the organization grows; so must the individual employee. When individual development is widespread throughout the organization, it becomes organizational development. Experience acts as a catalyst in the development process, bringing together the knowledge of education and the skill from training to make the employee a better performer. With development, the employee actually evolves into a different performer. This is important as developing the competencies of current employees are significantly less expensive than hiring new ones. Organizational development also enables the organization to provide more and better services to both internal and external consumers.

Each one has its place within the HRD process and although related to each other, each is a separate, distinct entity. Moreover, each process has differing effects on performance. Training will have a readily identifiable, measurable impact on job performance (provided the training is properly given), whereas education will change attitudes and outlooks (affective domain). Job task performance changes may not be as readily discernable with education.

"The Definitional Dilemma" often occurs when managers provide educational opportunities for their subordinates and think that the personnel have been "trained." Examples include having a guest speaker talk, or sending subordinates to seminars and conferences. These experiences educate but do not train. The "Dilemma" hits when the manager expects the same performance changes with education as with training. The manager is disappointed that extensive performance improvement has not occurred where he sent his officers to a "training session."

In some extreme cases of "The Definitional Dilemma," experience is confused with training. The manager speaks about the training that his personnel have had, when in fact all that they have is experience. Experience is not the best teacher—it is the most expensive teacher; one can learn improper methods through experience and have them reinforced every time the method is used. In other words, "only perfect practice makes perfect performance."

Training, education, experience, and development are all separate entities. A smart manager understands this and uses these professional growth experiences to complement one another.

The Frog

"The Frog" is a nice fellow who really means to do some wonderful work in the training arena. He wants his officers to be well trained. "The Frog" does not see the complexities and problems inherent within the training process. He jumps into training without thinking through all of the logistical considerations:

- Training needs assessment
- Training program development costs
- Equipment and materials needed
- Scheduling and overtime considerations
- Testing and validation methods

"The Frog" enthusiastically jumps into training, then crawls out of it when logistical hurdles appear. The training effort is abandoned for all practical purposes and professional growth is stopped. Often, this occurs when a new manager takes over. In some security organizations, this has happened repeatedly over the years. The senior security officers have lived through several administrations that were going to have good, strong training programs. In all likelihood, they will out-last the current "Frog." Small wonder that the security officers do not take training seriously!

"The world was not built on good intentions."

Popular saying.

The Panacea

Those who subscribe to this theory believe that training can solve any and all personnel performance problems. Personnel who have not been trained cannot be expected to perform. But training cannot solve all performance deficiencies. Training can only address problems resulting from deficiencies in skill, knowledge, or ability. Unfortunately, job performance inadequacies can also be the result of people not being motivated to perform, being prevented from performing due to some real impediment in the job design, or not knowing how to perform. Training can solve some performance problems; the overwhelming majority call for creative, no-nonsense supervision and management.

Some steps that can be taken to more accurately diagnose the performance problem include the following:

- Describe the problem by writing a problem statement in specific terms.
- Conduct a job task analysis so that there is a clearer picture of the total job environment.
- Determine the cause or causes by asking job incumbents and supervisors what they believe the problem to be, reviewing the appropriate metrics.
- Ask if the problem can be addressed through an increase in knowledge, skill, or ability.

Bad Medicine

"Bad Medicine" is the prescription of training for problems that training cannot solve. There are two varieties of it; the first being the manager, who uses training in a punitive manner. Training and discipline do not mix! Training can, to some extent, be a motivator. Motivation can be thought of as the "flip side of discipline"—part of the same "record," but a separate and distinct "song."

"Bad Medicine" hurts the organization by spending money foolishly. It can destroy the image of the training department by utilizing training in cases where discipline would be appropriate. This leaves a bitter aftertaste in the mouths of all involved and is certain to cause employees to view training in a punitive, negative light. Unfortunately, in some organizations labor–management relations have been allowed to degenerate into such a state.

The second common manifestation of "Bad Medicine" relates to the individual, who seeks out instruction in various topical areas and uses it for correcting personal deficiencies. It is not uncommon to find trainees who have taken innumerable classes and are not moving ahead in their careers. Some of these people have advanced degrees, certifications, etc. On paper they appear to be qualified; but in reality they lack something. They take classes but do not improve because the additional instruction is not addressing the root cause of the problem. This may be a personal deficiency, personality trait, or lack of aptitude in a particular area. The individuals doing this usually have facilitators helping them along.

Such a practice is common in employment and educational environments. It is a simple, convenient, unethical, and ultimately cruel response to problem employees and students. Managers, trainers, and educators have a professional responsibility to be honest with their charges and prescribe appropriate solutions.

The Assessment Ass

"The Assessment Ass" is not really serious about training. "The Assessment Ass" assesses and examines various training strategies, plans, and programs. Typically these are complex, sophisticated, and trendy ventures. "The Ass" is identified by the telltale statement:

"We're assessing...."

The strategy, plan, or program that is being assessed sounds very impressive. In fact, it is very impressive! A manager who would utilize such a strategy, plan, or program would be doing something outstanding, taking training steps that the security industry could emulate.

Sending all of the officers to a federal training center sounds great. Having all security personnel given 40 hours of classroom instruction is laudable. Using big-name instructors is wonderful. So is entering into a joint training venture with a local community college. Videotaping and critiquing all students on task performance is a marvelous idea.

All of these things sound wonderful. Unfortunately, in the vast majority of cases, none of them will become a reality. There are, after all, roadblocks that must be overcome:

- Budgetary limitations
- Scheduling shortcomings
- Availability of learning resources such as equipment, instructors, and facilities

Therein lies the problem with "The Assessment Ass": these brilliant ideas are not likely to happen. And "The Ass" knows this or at least should know it. "The Ass" is either deliberately trying to mislead others or is simply too inept to realize that money does not grow on trees.

The Budget Buster

This is when a manager has his/her subordinates attend a training program, generally put on by an outside consultant. In most cases, the outside consultant impresses management greatly. When all the costs of the training are calculated—often after the training has occurred—it is found that there is no more money for training left in the current fiscal year. Having the officers undergo the training is not the problem, assessing costs and performance outcomes is. Before embarking on any training initiative, managers must cost out the initiative. This is especially true with "one-time shots." If a program is going to exhaust the budget, it must be worth the price. Managers must be aware that only so much learning will occur within a given time period. While this varies widely with differences in instructional design and delivery, there is a real limit to what will be learned. One rule of thumb that is good to use is that in a 4- or 8-hour class, a participant will learn three to five things that will be useful on the job.

Generally speaking, large budgetary allocations should be directed toward programs that are comprehensive and continuous. Sending the staff through the CPO program or buying a subscription to the Private Security Training Network are examples. Both programs cover numerous subjects, are continuous, and provide for testing and evaluation of learning.

In cases where expensive, one-shot programs are unavoidable, the learning experience should be made as continuous as possible. Pre- and postwork should be utilized. Having the class participants read and study the topic before the class is an option. Another is to have them work with the information that has been learned at the end of the class. This can take many forms such as teaching a short class on the topic to others, changing a procedure, or simply personalizing it into their jobs: "What will you change about the way you do your job?"

Roleaids

The "Roleaids" manager fails to appreciate the role and function of the contemporary protection officer. Briefly stated, in very simple terms, the role of security officers includes the following components:

1. Intelligence agent for management via the collection of information that management needs
2. Enforcement/compliance agent for management policies
3. Management representative through the enforcement of rules and the providing of information and directions to visitors, employees, and customers
4. Legal consultant where the officer has a working knowledge of more areas of the law than any other member of the organization (labor law, administrative regulations such as OSHA, criminal law, and civil liability standards)

The "Roleaids" manager does not understand this. He thinks of security officers as "guards." As a result he does not develop his subordinate officers. The officers are not socialized as adjunct members of the management team. They are not given the human and public relations training necessary to interact with others in a productive manner. Their interpersonal communication skills are not honed so that they can "sell" people on policy adherence. Writing skills are not developed to enable them to record data efficiently.

The solution to "Roleaids" is to have the afflicted manager study security officers in some manner. He must become educated about what the officers do. Reading the relevant ASIS Guidelines would be reasonable start. Another, more organizationally relevant learning experience, would be to conduct a job task analysis. A compensation review by a human resources specialist is something that can aid this—and it should probably be done periodically anyway. Having the manager spend some time with the officers can also be a help. Getting the manager to write a few paragraphs defining "security officers" can be a key to solving this syndrome. Giving the officers a change in job title to more accurately reflect what they do can also help. This may serve to solidify what new information has been uncovered.

Toad Training

"Toad Training" is an occasional occurrence in the security industry. It takes place when security officers with limited cognitive ability are hired and trained. Assuming that a professional training program is in existence; management will inevitably be disappointed when the new recruits graduate as there will be an abundance of well-trained "toads" in the workplace! These employees simply do not have the judgment or communication skills necessary to be effective protection officers.

These employees are not the best ambassadors for the organization! There is no excuse for hiring substandard personnel—especially when those employees are representing the organization. Unfortunately, it happens on occasion due to a gross and perhaps deliberate misunderstanding of the duties and functions of security personnel (see "Roleaids"). Training is a part of HRM. It is not completely separate from selection, recruitment, supervision, motivation, etc. Trainers must assume the role of consultant rather than hiding within the confines of the classroom. They must become involved in the overall HRM process including selection, recruitment, and evaluation.

Mr. Unique

"Mr. Unique" perpetually resists purchasing off-the-shelf training programs because they are generic and not specific enough to his/her work environment. He magnifies the differences instead of linking the similarities between his organization and others. "Mr. Unique" thinks that his/her problems are like no other. As no off-the-shelf training program addresses these problems—in his mind—he does nothing regarding training. Note that "Mr. Unique" is usually very convincing in his arguments.

"Mr. Unique" fails to see that such issues as negative public relations, poor human relations, inadequate reports, sloppy investigations, and ineffective enforcement are problems shared by the entire security industry. Rather than learn from other managers, professional organizations, and off-the-shelf training programs, he does nothing. He retreats from addressing the problem under the guise of his situation being unique and therefore, unsolvable.

"Mr. Unique" is often very convincing in his arguments! He can be dealt with by assessing the following questions:

1. What training program is currently in place?
2. What training program is desirable in the near future?
3. What would it cost in personnel's time and consulting fees to develop a tailor-made training program?
4. How much budgetary support is currently available?
5. What will the results of failure to train personnel be in a year from now? Two years from now?

Marketing

"Marketing" occurs when an impressive instructional program is portrayed to a client or other key decision maker. It is represented that the security force is going through this impressive-sounding instructional process. Computer simulations. Attendance at a federal government training class. Participation in a full-scale scenario exercise. In reality, only a few select persons go through it. It is sort of like the classic "Bait and switch" in fraudulent advertising. It can, however, be managed through asking the key question concerning contact: the amount or percentage of persons who have undergone the learning experience within the organization. A key aspect of evaluating training in terms of organizational development is contact. The manager must always know how many or what percentage of the protection force is actually going through the training.

The Profiteer

This is an unethical firm or individual, who takes advantage of misinformed students and in some cases government grant monies. "The Profiteer" misrepresents instructional programs. Students are suckered out of their tuition monies with the promise of careers that are essentially unattainable.

In the United States, during the 1980s, this was in the form of Pell grants for training economically disadvantaged persons. Some of these individuals had criminal records that would preclude their employment in security. Others were enticed to spend their own money on the training. These students were told of fantastic careers as FBI and CIA agents; television ads showed Personal Protection Specialists in suits with automatic weapons rappelling out of helicopters.

In the not too distant past, private training schools took advantage of the popularity of the CSI television show. Ads focusing on possible careers as crime scene investigators began to appear. "The Profiteer" may appear in states or provinces where training is mandated, taking unfair advantage of poorly written and implemented training requirements. The syndrome will take different forms in different areas and different times. Instructional processes cost money and time. They must be professionally designed and delivered so that all stakeholders may benefit. Unfortunately, there are always those who are unethical. There are always those who do not "tell the truth, the whole truth and nothing but the truth."

Conclusion

Supervisors and managers play a crucial role in the training process: in the final analysis they are what makes the training process work!

By learning as much as possible about learning theory and delivery, supervisors can significantly enhance their contribution to officer performance. They will also expand their own career potential and increase their value to themselves, their families, their employers, the security industry, and society. Training and developmental programs in contemporary protection organizations must be dynamic and multifaceted. While protection staff is the primary focus of developmental efforts, customers, clients, and employees are also potential training recipients. These latter groups may become a major part of a security or loss prevention departments focus. There may be situations where the protection department acts as a training provider to other departments. There may also be revenue generating opportunities should the department offer instructional services outside the parent organization. Simply stated, protection supervisors have a substantial role to play, a role that is expanding.

In order to fulfill this role and be a major contributor, protection supervisors must understand and be able to apply learning strategies. They must know what needs to be learned and how to best facilitate that learning. They must become perpetual students of training and development. They must understand that learning never stops. And they should exploit every opportunity to see that it occurs.

Endnotes

S. Albrecht (2006). *Tough Training Topics: A Presenter's Survival Guide*. San Francisco, CA: John Wiley.
L. Brockelsby (1986). "Good In-Service Training: The Chiefs Perspective." *The Police Chief* LII(11).
S. M. Bunting (1993). Training Safety: A Supervisory Responsibility *In* "Supervisory Survival" (E. Nowicki, Ed.). Powers Lake, WI: Performance Dimensions Publishing.
Ginny Field (1993). Supervisory Editing. *In* "Supervisory Survival" (E. Nowicki, Ed.). Powers Lake, WI: Performance Dimensions Publishing.
R. B. Frantzreb (1990). *Training and Development Yearbook*. Englewood Cliffs, NJ: Prentice-Hall.
D. M. Grossi (1993). The Supervisor's Role in Officer Survival Training. *In* "Supervisory Survival" (E. Nowicki, Ed.). Powers Lake, WI: Performance Dimensions Publishing.
C. A. Hertig (1993). *Avoiding Pitfalls in the Training Process*. Bellingham, WA: International Foundation for Protection Officers.
K. I. Minor, R. W. Snarr, and J. B. Wells (1998). "Distance Learning: Examining New Directions and Challenges For Criminal Justice Educations." *ACJS TODAY* 16(4).
R. Metzner (2006). "Training's Return On Investment: Don't Prove It, Find It." *Loss Prevention* 5(6).
H. C. Mounts (1997). "Earn Your College Degree At Home." *Police and Security News* 13(1).
L. Nadler (1970). *Developing Human Resources*. Houston, TX: Gulf.
D. A. Nichter (1997). "How MGM Grand Trains Security Officers, Supervisors, Managers." *Hotel/Motel Security and Safety Management* 15(8).
C. Nilson (1989). *Training Program Workbook and Kit*. Englewood Cliffs, NJ: Prentice-Hall.
Barbara E. Roberts (1993). Supervisory Liability. *In Supervisory Survival* (E. Nowicki Ed.). Powers Lake, WI: Performance Dimensions Publishing.
J. A. Sample (1983). "Police Performance Problems: Are They Training Or supervision Issues?" *The Police Chief* L(10).
C. A. Sennewald (1985). *Effective Security Management*. Stoneham, MA: Butterworth.
B. Siuru (2007). "NACHS—A One-Stop Shop for Homeland Security Information and Training." *Police & Security News*. 23(1).
K. Tyler (2005). "Training Revs Up." *HR Magazine*. 50(4).
J. A. Wanat, E. T. Guy, and J. J. Merrigan (1981). *Supervisory Techniques for the Security Professional*. Stoneham, MA: Butterworth-Heinemann.
R. Zemke, L. Standke, and Jones, P. (1981). *Designing and Delivering Cost-Effective Training—and Measuring the Results*. Minneapolis, MN: Lakewood Publications.

FOR MORE INFORMATION

Advanced Systems Technology offers a myriad of online and CD-ROM programs for law enforcement, telecommunicator, first response, and security personnel. AST provides the online learning for the Federal Law Enforcement Training Center. They also have a whole series of programs for continuing professional development. Members of the International Foundation for Protection Officers (IFPO) receive a discount on these programs. Contact hits@astcorp.com

Butterworth-Heinemann is an imprint service of Elsevier (www.elsevier.com). Butterworth-Heinemann has been the premier publisher of security texts for several decades. There are numerous titles to choose from including textbooks on Training, Management, etc.

The International Association of Law Enforcement Educators & Trainers (IALEETA) (www.ileeta.org) is an organization for those involved in teaching law enforcement and criminal justice. IALEETA has an extensive array of membership benefits for instructors and sponsors on outstanding annual conference each year.

IFPO (www.ifpo.org) offers an array of online and printed learning options. Membership in the Foundation provides substantial discounts on IFPO offerings as well as those of affiliated organizations. The Certified Protection Officer Instructor (CPOI) program

prepares individuals to conduct the CPO program in a traditional classroom environment. It also affords the candidate with a recognized instructional credential.

The National Academic Consortium for Homeland Security (NACHS) (http://homelandsecurity.osu.edu/NACHS/) has information relating to Homeland Security as well as a listing of degree and certification programs.

Dr. Steve Albrecht has written an outstanding book entitled *Tough Training Topics: A Presenter's Survival Guide*. The book offers numerous tips on presenting programs as well as program outlines on performance evaluation, sexual harassment, substance abuse, and other key areas. The book is published by Pfeiffer, an imprint of Wiley (www.pfeiffer.com).

The Professional Security Training Network (PSTN); (800/942-7786 or http://www.twlk.com/security/) offers hundreds of videos for the professional development needs of supervisors and officers. There is a monthly subscription service where subscribers receive a new program each month as well as tape series on specialized industry sectors. The videos and other media come as complete instructional programs with examinations, etc. Certificates of completion can be printed online. PSTN also produces the Basic Security Officer Training Series. This instructional package provides a comprehensive introduction for preassignment training. Members of the International Foundation for Protection Officers receive discounts on PSTN programs.

The Office of Community and Professional Development at York College of Pennsylvania (www.ycp.edu or 717/815-1360) hosts a variety of programs dealing with security-related topics at York as well as offering courses at client locations. Online Learning Options for the Security Supervision and Management Program, the (CPO) Program, and the Crime and Loss Investigation Program are available. Information on Careers and various security industry topics in the form of Practice Examinations and Tutorials available at http://goose.ycp.edu/~chertig.

Training: Strategies, Tactics and Challenges for Protection Managers

Quiz

1. Supervisors who are charged with training their subordinates must ensure that the training is _____.

2. There are numerous problems in the _____ development and implementation of training.

3. _____ education, which offers learners the opportunity to work at their own place and their own time, is key to delivering instructional programs.

4. _____ training occurs when training is done only to satisfy government regulations.

5. _____ is an essential instructional technique for teaching proficiency in areas such as equipment use.

6. Job aids serve as reminders as to how to perform a certain task, such as operating a piece of equipment. ☐ T ☐ F

7. If one uses a distance education approach to teach policy and procedures, reinforcement in the classroom or via individual meetings is not necessary. ☐ T ☐ F

8. Tuition reimbursement is widely used and fully exploited by most security employers. ☐ T ☐ F

9. When editing a subordinate's reports, the supervisor should praise, question, and polish. ☐ T ☐ F

10. Security supervisors, particularly in the "private sector," will probably be held liable for the lack of training given to their subordinates more often in the future due to the increased responsibilities and public contact on the part of private protection forces. ☐ T ☐ F

2 Orientation for Security Officers

David H. Naisby

Introduction

Orientation begins prior to the effective date of employment, prior to communicating the corporate benefits package, and prior to introducing your new hire to organizational staff members. "Orientation of New Employees" begins with the posting of a vacancy, the invitation to enter the employee screening process, and most importantly—the interview itself.

Technically speaking, the orientation of new employees begins when the applicant reports for their first day of employment. The mood should be light, the atmosphere comfortable, and the anticipation of beginning a new relationship (for both parties) be one of enthusiasm rather than anxiety, paranoia, or distress. Taking appropriate measures during the marketing and selection process will help to set the foundation for a marriage between your corporate objectives and your employees' desire for success.

On or before the first day, it is suggested that new staff receive a thorough orientation to their new job and the institution for which they will be working. In this way, they will get a good impression of the employer, and the supervisor/instructor will provide them with the initial information and tools they need to be successful.

What follows is a list of activities and/or topics that should help new staff become productive colleagues. Each organization should tailor this list to represent their unique business objectives, and decide who in the organization will take responsibility for each item.

In this chapter, you will learn about measures that should be considered prior to the selection process as well as critical components that will help you plan for a seamless transition into your institution. More importantly, you will learn about key review process that must be taken as part of an ongoing corporate orientation program, and you will learn about performance measures that will help assess the effectiveness of your orientation program.

Preorientation

Interviewing 101—"Make a good first impression." Your new employees remember the cliché, their career path has been overshadowed by how they present themselves throughout their interviewing process. They realize that all first impressions, especially the interview, are critical. While the applicants' first impressions establish a foundation for everything that follows during their interview process, the security supervisor must also consider that the candidate is also forming an impression of the supervisor and the institution.

With this in mind, you must be cognizant of how you portray yourself, your bureau, and your organization. How you communicate, both verbally and nonverbally, leaves a lasting impression in the mind of the applicant. It is critical that you recognize this fact when publishing position vacancies, position descriptions, scheduling interviews, and when meeting with the applicant for the first time. Your organization depends on you to represent the agency's interests and to portray a positive image at all times.

Before New Staff Member Arrives

New employee orientation should begin with ease and transition for both the employee and the institution. In order to make that connection, however, it is imperative that all facets of integration are utilized. With respect to the embracing of a new employee, current staff and the prospective newcomer should be aware of their roles as well as those complementary to them.

The new employee should review and become familiar with their job description. This job description should specifically explain how the officers should perform in the organization. It should include control and planning tasks and system-wide obligations. The direct authority for the employees should also be identified to prevent conflicts arising from uncertainty as to who makes the decisions for particular issues. The job description should also reflect the organization's expectations of employees regarding self-management responsibilities, and should include temporary job assignments that may happen during employment.

Recommended steps for you to take prior to the new employees' first day of employment include sending the new staff member:

- A welcome letter
- A job description
- Instructions for first day and week
- When, how, and where to arrive
- Who to ask for and a direct telephone number
- Where to park
- Suggested attire
- What to expect for the first few days
- Orientation/introduction to people, job, office, department, and the organization
- What to expect regarding meals, breaks, and time for personal business
- Initial work responsibilities
- Required or recommended reading, such as any publications created by your department
- A description of the work setting
- Other advance preparation

For current staff, you should consider the following elements as part of their orientation to the new staff member:

- Distribute an announcement to current staff
- Schedule time for all staff to meet the new employee; block time for essential meetings with payroll, personnel, supervisor, etc.
- Communicate the new employees' role in the organization
- Why the candidates were selected and a list detailing their experience/value they bring to the institution
- Disseminate a photograph if possible
- Get them to know the new officer

First Day of Work

At the start of the first day, each new employee shall have a payroll and personnel orientation. The orientation is designed to help new employees better understand personnel policies and procedures. The session should last 1 hour and will review general payroll and personnel topics such as meeting the payroll/personnel team, pay rate and schedules, benefits, performance evaluation and standards, holiday schedules, etc.

Additional checkpoints for the first day should include:

- Issue an employee ID. Nothing says "Welcome to the Team" like a new badge with your employees' photo, name, and corporate logo
- Meet with the employees' supervisor (and others as appropriate) for office orientation, goals, and objectives
- Review primary activities

- Communicate policies, procedures, bulletins, and other governance documents such as:
  - Working hours
  - Telephone techniques and etiquette
  - Correspondence styles
  - Staff meetings
  - Budget and accountability
  - Service culture
  - Confidentiality
  - Ethics
  - Working with supervisors, colleagues, assistants, and/or volunteers
  - Managing office conflicts
- Review and discuss questions about job description and evaluation criteria
- Introduce the employee to their designated work space/office (if appropriate)
- Meet with colleagues and support staff, and provide a brief overview of their responsibilities and assignments
- Meet with assigned support staff (if appropriate)
- Explain office organization (files, supplies, etc.)
- Discuss procedures for handling incoming and outgoing mail and office circulation files
- Indicate the location of office resources (directories, dictionaries, style manuals, computer program manuals, staff listing, etc.)
- Demonstrate how to use your telephone equipment
- Review office dress code
- Indicate where to put coat and personal belongings
- Show the employee the location of restrooms, refreshment area, and lounges
- Discuss procurement processes and how to obtain office supplies
- Review:
  - Refilling paper supply
  - Policies about number of copies and making personal copies
  - Fax machines
  - Calendars
  - Coffee/coffee fund, gift fund
  - End-of-day routine: lights, telephones, doors, computers, etc.
  - Where to go for lunch, dinner, or breaks

Because of financial, personal, and legal implications, a lunch companion should not be a formal part of the schedule if lunch is not a reimbursable expense. The new employee should not feel obligated to eat lunch with staff in the event that they feel they cannot afford it, or if they need the time for personal business. Let your new staff member have some breathing room.

Other Points to Consider

It would be valuable to assign a "partner" to a new staff member, preferably a peer from the office area, to whom the new employee can ask any question without fear of reprisals. A colleague who is relatively new to the organization might be the best choice because they have a fresh perspective and they are familiar with questions a new staff member might have. If a "partner" is not assigned, someone else should cover these topics with your new staff member.

Mentoring is a formal process where mentors who are trained and sometimes compensated for taking someone under their wing. Mentors are generally senior employees who can provide both an example to the new employee and address any concerns that they might have.

Mentors are not supervisors. They perform no evaluative functions. They may represent management insofar as proper codes of conduct and performance are concerned, but they have no authority to discipline.

Field Training Officers (FTOs) are similar to mentors in that they help to socialize the new hire into the job. FTOs differ from mentors in that they also evaluate the probationary employee. FTOs must be trained in how to teach/train/instruct as well as how to evaluate/supervise.

Within First Week of Arrival

If not completed on the first day, within the first week of employment, each new employee shall be given a departmental orientation by the immediate supervisor. The orientation will cover the department's functions, organization, and goals. Information given to the employee will also include job responsibilities, annual review, performance evaluation standards and expectations, introduction to department members, tour of department, confidentiality, and emergency procedures.

While all attempts to address these areas should be taken on the first day, you must keep in mind that overwhelming the employee can have the same affect as doing nothing at all. The immediate supervisor should address and readdress all of the following key components during the first week:

- Set up the employees' work area
- The supervisor should check in frequently to clarify expectations and answer questions that the employee may have
- Colleagues should also check in to answer questions and offer support
- A "partner," mentor, or FTO should check in daily to answer questions and offer support
- Meet with department business manager/payroll/personnel to cover, as appropriate, the following:
  - Time cards
  - Vacation/sick/personal leave policies
  - Keys
  - Access to the office on nights and weekends
  - Telephone: access code, personal calls, paying for personal long-distance calls
  - Stamps, parking permits
  - General review of accounting
  - Listing of account numbers
  - Journal vouchers
  - Travel and reimbursement (especially for business travelers)
  - Company credit card
  - Telephone credit card use (saves money over paying the full rate from a hotel room, for instance)
  - Cellular phones, pagers, personal digital assistants (PDAs), and BlackBerrys
  - Paying bills, making deposits, transferring between accounts
  - Meet with company human resource services
  - Complete all necessary paperwork
  - Review company personnel policies and procedures
  - Learn about and submit benefits (health and life insurance, retirement, select benefits, etc.)
  - Learn about company orientation
  - Get company ID (highly recommended on first day)
  - Get company parking permit (if appropriate)
  - Meet with management information systems (MIS) personnel for computer assistance, network access, e-mail, and policies. Assess knowledge of and comfort with computer hardware and software and schedule training if necessary.
  - Overview of policies and procedures, including confidentiality and piracy
  - Hardware: turning on, backing up, printing, shutting down, etc.
    Software: word processing, data processing, e-mail, etc. as needed
  - Tour the building and immediate area

Within 6 Months of Starting

- Meet key people and offices within the company
- Meet on a regular basis with supervisor to discuss issues, and review job description, expectations, and performance

- "Partner/mentor" should continue to check in on a regular basis to answer questions and offer support
- Attend company's new staff orientation (provides an overview of company people, departments, policies, and procedures, and includes a tour of the company facilities)
- Have 90-day and 180-day performance review

Performance Measures and Program Evaluation

Orientation is a critical juncture in socializing the new employee. It "marries" recruitment, training, supervision, organizational attitudes, and personal characteristics into one consolidated impression. Due to the significant importance of first impressions, the "reality" of present day security force training, and the critical element of understanding of the organizational culture by protection officers, orientation must be carefully programmed and regularly evaluated for effectiveness.

Implementing a review of your success should be part of every professional's personal assessment. As all professionals should effectively pursue opportunities to continuously improve, so should the image of our organization. While self-evaluation is highly recommended, all recruiters, mentors, managers, and staff should regularly evaluate their orientation programs for both success and opportunities for improvement.

Orientation for Security Officers: Chapter Review Questions

1. Orientation of new employees should begin when?
   (a) Once a worker is familiar with his/her position
   (b) The first day of work
   (c) Upon initial contact with a prospective employee
   (d) When management feels the time is right

2. New employees should familiarize themselves with their job description when?
   (a) When a "buddy" is assigned
   (b) During the hiring interview
   (c) It should be taught on the job (OJT)
   (d) Before the first day of work

3. The "buddy" system is useful because:
   (a) It takes pressure off the supervisors in the organization
   (b) Experienced employee can provide useful information without fear of reprisal
   (c) Employees can become friendly early in their career
   (d) Many organizations have employees with nothing else to do anyway

4. When should a new employee be introduced to the organization goals, functions, and philosophies?
   (a) During the hiring interview
   (b) Within the first week of arrival
   (c) Never, it should be something the new employee will inherently pick up
   (d) The first day of employment
   (e) All of the above

5. The first day of work should include:
   (a) Understanding where your work space should be
   (b) Meeting with colleagues and support staff
   (c) None of the above
   (d) All of the above

6. When is the "buddy system" necessary?
   (a) Throughout an employee's career
   (b) Until the new hire feels comfortable in his/her position

(c) Only in the first week of work
(d) During the first month of employment
(e) None of the above

7. Scheduled "Performance Dialogues" are important because:
   (a) The employee will know when he/she is eligible for benefits
   (b) The institution is obligated to evaluate the employee
   (c) It is an opportunity for the organization to evaluate and comment on work performance
   (d) It is an opportunity for the employee to be introduced to new philosophies

8. Every institution should have an orientation policy.
   (a) True
   (b) False

9. New employees are required to complete performance measures.
   (a) True
   (b) False

10. Make sure that
    (a) New employees understand their new environment
    (b) The "buddy" documents every action of the new employee
    (c) You explain any reorganization or job restructuring to the current employees necessitated by a new hire
    (d) All of the above

3

Staff Training and Development

Charles T. Thibodeau

Training is the bedrock of a balanced, stable security force. A well trained security force is more likely to provide required services, in an effective and efficient manner, free of legal liability. The officers operate both as a well-orchestrated team and as effective, independent "can do" service personnel. They are usually very visible, approachable, and seem always to be in the right place at the right time. They make a positive impression on the people who work at or visit the owner's property.

From a legal perspective, if the company is ever sued by a plaintiff for injuries resulting from a claim of inadequate security, in addition to charges of negligent hiring, negligent supervision, negligent retention, negligent entrustment, and negligent assignment, it is likely that there will also be a charge of negligent training. That is, the plaintiff will charge that either the company failed to provide training, the training that was provided did not meet some standard, or the trainer was not qualified due to lack of experience and/or proper credentials.

Some settlements reported in the Association Trial Lawyers of America law reporter (ATLA Law Rep.) related to the negligent training issue include: a $1.25 million award for inadequate training in proper security measures, 32 ATLA Law Rep. 366, October 1989; a $100,000 award for negligent training in an assault and battery case, 30 ATLA Law Rep., 272, August 1987; a $12.3 million award for negligent training of employees who improperly used monitoring equipment, 30 ATLA Law Rep. 262; a $4.2 million award for failure to teach the use of alarms, and failure to provide a trained and adequate security force, 32 ATLA Law Rep. 20, February 1989; and finally a negligent training award of $500,000 for a wrongful death of a shoplifting suspect who was shot by a guard, 29 ATLA Law Rep. 39, February 1986.[1]

In order to properly protect a company from legal liability, it is important to ensure that security personnel receive "adequate training" by training the trainer before they are allowed to instruct. One of the greatest mistakes made in the training of security personnel is the use of an untrained instructor. In a lawsuit, one of the first questions that the plaintiff's attorney will ask the trainer is, "please describe all of your education and experience that qualifies you to be a trainer of security personnel" or words to that effect. Unfortunately, in most cases the trainer has no credentials and the plaintiff's case for inadequate training is made. This chapter will provide some direction for putting together an effective training and development program for your security department.

Three Domains of Training

First of all, it is important to realize that there are three domains of training: cognitive, psychomotor, and affective. A balanced training program will contain all three. The cognitive training

[1] David A. Maxwell (1993). Private Security Law. Boston: Butterworth-Heinemann, p. 407.

domain is most often taught in a classroom and is usually known as preassignment training. Cognitive training tackles theory and knowledge and is usually presented using lectures, demonstrations, video presentations, illustrations, readings, tutorial exams, and homework.

In many companies the training process is short-circuited at this point by the exclusive use of short videos without an instructor. No one can receive adequate training by merely watching some generic videos about security. It will be extremely difficult for a defense attorney to prove adequate training once the plaintiff's attorney has discovered that all the security officers received by way of cognitive training was 6 hours of videotapes.

Psychomotor training is the hands-on part of the training process. This is usually taught at the job site and consists of such things as facility orientation, patrol techniques, equipment training, emergency response, and department-authorized security procedures. In many companies this is the only training security officers receive. In fact, often the company will send a new recruit out to a facility for 15 or 20 min of training before their first shift. In other words, after 15 or 20 min of training the multimillion dollar building is turned over to the new recruit.

In many cases companies assign new security officers to work with experienced officers for 2 or 3 days before they are allowed to take on their own shifts. Three days or more of preassignment or on-the-job training, in conjunction with at least 12 hours of cognitive classroom training will make it much easier for the company's attorney to defend the position that the company provides adequate security officer training.

Affective domain training covers work values and/or professional attitudes. The danger here is that values are automatically and inadvertently being taught by everyone, all the time. The way we dress, our mannerisms, our statements about race, religion, sex, everything we say or do is continually communicated. Our audience, those we communicate with, as well as uninvited listeners, are subjected to our values and attitudes whether we want them to be or not. Our listeners are influenced by our values and attitudes, especially if the listener has great respect for us as teachers, instructors, or trainers.

It is important for the trainer to be aware of affective domain training and to include some specific work-related values and attitudes in both the cognitive and psychomotor lesson plans. The way these values and attitudes are delivered is different than the cognitive and psychomotor training. Values and attitudes are not taught as separate subjects, but are linked to the other two types of training. The trainer must be prepared to inject the appropriate value or attitude whenever the opportunity presents itself.

The trainer who comes to work in an unkempt uniform will have a difficult time training others to wear their uniform with pride and to take care of their appearance. The male trainer with long hair and an earring in his ear will have a hard time convincing male students that they must wear their hair short and not wear earrings. If the trainer comes to class late all the time it will be hard for the trainer to criticize tardiness or teach the virtues of being punctual. If the trainer does not follow the sexual harassment, diversity, and multiculturalism guidelines of the company, the students will likely have problems in those areas as well. It is not enough to teach in the affective domain; to be believable, the trainer must live this part of the training.

Training Program Development

There are four stages of training program development:[2]

1. Identifying the objectives
2. Designing programs to meet the objectives
3. Organizing the programs to meet the objectives
4. Evaluation of the programs in terms of the objectives

Each stage is separate but related to the other stages. At each step decisions have to be made and problems solved. Throughout the analysis it is important to keep in mind the cost-effectiveness

[2] Ivor K. Davies (1981). Instructional Technique, New York: McGraw-Hill Inc., pp. 10–11

of the training program. In most cases, the determining factor of whether or not you will have a training program is your ability to prove to upper management the cost-effectiveness of your training proposal.

Identify the Objectives of the Program

What are the objectives of the program? Here it is necessary to decide on goals for the training programs which will directly address the real or perceived needs of the company. Review security officer job descriptions and requests for security assistance made by department heads in the company. Review daily activity reports, 911 reports from the public law enforcement and security and safety incident reports to determine threat levels and probability facts. Review the mission statement for the company and department. Prepare objectives to which the upper management, those who have to sign off on the training program, can relate. To do this you may want to survey top management to test their attitude and perceptions of security.

You must be able to clearly define what it is that you want the security officers to be able to do after receiving the training, and to what level you will set your expectations. Consider the following as a general guideline of desired outcomes. The trained security officers should be able to:

1. Observe, report, and take limited action.
2. Act reasonably.
3. Perform their duties within the civil law, criminal law, administrative law, company policies, and department procedures.
4. Exhibit high ethical standards.
5. Be a "can do" company servant.

We commonly find that expectations regarding the performance of security officers include the ability to perform certain skills, to obtain general and specific knowledge of the job and exhibit the proper work values and attitudes.

Design the Program to Meet the Objectives

The program content should include, but not be limited to, the following:

1. General: There will always be a need for cognitive classroom training. This training will carry a standardized curriculum, hopefully containing what every security officer needs to know about security.
2. Structured on-the-job training (OJT): At some point the new recruit will need to participate in OJT. This should normally take place after the classroom training, but it does not have to. As long as the cognitive training is completed within the first 21 days of employment, the OJT can take place first. Since the OJT and cognitive training are fully articulated, each type of training will strengthen and support the other. However, the OJT should be "structured" OJT not just "warm body training."

All security officers should know how to write field notes, how to write a report, how to respond to all emergencies relative to a particular work site, how to do foot patrol as well as vehicle patrol, how to run all of the equipments and systems including alarms, CCTV systems, card access systems, guard tour systems, fire panels. The officer should be highly skilled in human relations, know how to deal with the press, have a professional telephone manner, and know how to serve the needs of the people who inhabit the facility to which the officer is assigned.

In some settings the officers must know about the use of force, how to handle a variety of weapons, hand-to-hand combat, handcuffing, and the law of arrest. The list of information required goes on and on. It is for the trainer to determine the essentials. At the same time, the trainer must keep in mind cost-effectiveness and the need to satisfy tort law with regard to potential negligent training claims. Be sure that your course content is short enough to be cost-effective but comprehensive enough to defend against charges of negligent training.

What should be Included in the Curriculum

Although there are no national standards in private security, by comparing lawsuits over the past 10 years, we have attempted to determine what a standard might look like if one did exist. The following are some ideas for your consideration, given that you are about to train an unarmed security contingent:

1. Basic security overview
   2 hours
   (a) Role of the security officer
   (b) Typical assignments and "can do" service
   (c) Facility orientation
   (d) Patrol techniques
   (e) Access control
   (f) Reasonable observation
   (g) Reasonable reporting
   (h) Limited actions
   (i) Proactive prevention versus reactive security
   (j) Liaison with public law enforcement

2. Legal powers and limitations
   2 hours
   (a) Acting under "color of law"
   (b) Limited immunity versus no immunity
   (c) Tort law
      – Negligence
      – Intentional torts
      – Strict liability
      – Contract law
      – Imputed liability
      – Nondelegable duties
      – Selected case law
      – Merchant privilege laws
      – Defenses
      – The "reasonable person test"
   (d) Criminal law
      – Arrest and detention
      – Search and seizure
      – Burdens of proof
      – Probable cause
      – Reasonable suspicion
      – Defenses
      – Crime identification
   (e) Administrative law
      – OSHA Occupational Safety and Health Admin.
      – ADA American's with Disabilities Act
      – NFPA National Fire Protection Agency
      – EPA-HAZMAT Environmental Protection Agency-Hazardous Materials
      – EEOC and AA Equal Employment Opportunity Commission
      – Workers' comp. laws
   (f) Constitutional law
      – Miranda warning
      – Mapp versus Ohio
      – Burdeau versus McDowell

(g) Use of force
(h) Alternatives to the use of force
(i) Defensive weapons identification and use

3. Emergency response
   2 hours
   (a) Know the company policy
   (b) Know and practice the department procedure
   (c) Know how to identify an emergency
   (d) Know when to call 911
   (e) Know how to respond to fires
      – Low building fires
      – High building fires
   (f) Know how to respond to medical emergencies
   (g) Know how to respond to severe weather
   (h) Know how to respond to criminal acts
   (i) Know how to respond to bomb threats
   (j) Know how to assist public service personnel
   (k) Know how to deal with violence in the workplace
4. Safety and accident prevention
   2 hours
   (a) Observing and reporting unsafe conditions
   (b) Identify accident hazards
   (c) Identify fire hazards
   (d) Identify hazardous materials
   (e) Know the safety rules and regulations
   (f) Know how to respond to accident investigations
   (g) Know how to respond to report accidents
   (h) Maintain certifications in first aid and CPR
5. Report writing
   2 hours
   (a) Why write a report
   (b) The importance of note taking
   (c) Elements of a report
   (d) Proper times, names, and locations
   (e) Giving physical descriptions
   (f) Facts versus opinions and assumptions
   (g) The importance of good penmanship
   (h) Changes to reports
   (i) Reports as legal documents
   (j) How to perform in court
6. Human relations
   2 hours
   (a) General public relations skills
   (b) Principles of good communications
   (c) Proper telephone procedure
   (d) Listening
   (e) Avoiding confrontation
   (f) Dealing with the media
   (g) Dealing with front line rage
   (h) Escalation de-escalation continuum
   (i) Escalation verbal de-escalation continuum
   (j) Breakaways to verbal de-escalation
   (k) Breakaways to escape

The above represents a model curriculum for an unarmed security officer contingent. This is only the author's concept of a model training program. There are many others that are just as good,[3] but this model incorporates all the author has learned from studying the errors of security officers and the lawsuits that have resulted. Armed officers and those who are issued defensive weapons other than firearms, would have to attend the above cognitive preassignment training in addition to firearms and defensive weapons training.

Organizing the Program to Meet the Objectives

When considering how to meet the "duty of care" by providing "adequate training" for your security staff, first determine if a contract program is available within your budget constraints. A good place to look for contract services is the local customized training departments of technical colleges and community colleges. This approach has a number of advantages.[4]

Most technical colleges can provide licensed or certified personnel to teach the curriculum; the college can prepare the curriculum, order textbooks or prepare handouts, administer and proctor final exams, keep training records, and, perhaps best of all, mitigate legal problems if your security officers are ever sued; that is, the plaintiff's lawyer may drop the charge of negligent training as soon as the lawyer finds out that training was delivered by outside professionals. In addition, your thoughtful decision to use a well respected educational institution in the community might help to show your company in a favorable light to the jury.

The one negative side of utilizing colleges for training is the cost. Customized training is much more expensive and the cost could easily exceed your training budget. However, it is well worth it to check out the cost of a college program before embarking on the creation of a proprietary training program. The Job Training Partnership Act (JTPA), underwrites the most important public programs currently being used to help employers with training activities. The financial aid departments of technical colleges and community colleges will have information regarding this agency. Some programs are controlled by the Private Industry Councils (PICs) and are funded by block grants to the state. If your budget is slim it would be worth it to check into these block grant programs.

Once it has been determined that your company is going to create its own proprietary training program, many logistical matters must be decided upon. These include, but are not limited to, the program's budget constraints, the location, and whether the program will be presented on-site or off-site, what materials are needed (such as audio-visual equipment, blackboards, lecterns, etc.), the program schedule, length of the program in hours (in terms of legal liability, what is the standard acceptable number of hours?), are you going to hire a consultant to help prepare the program, where are you going to get trained instructors, who in the department will be designated the official trainer, should you hire a trained and certified person from outside the department to train the officers, what training records you will be required to keep, who will prepare the curriculum (in terms of legal liability), what topics should be included in the training, how can you tie the cognitive domain training to the structured OJT portion of the program, and how will you evaluate the effectiveness of the program?

One of the most important considerations was not even touched upon in the above paragraph. The question is, "Is enough money in the budget to pay the security officers to attend the training?" If the company insists on having a proprietary training department, then security officers should be trained off hours and paid for their attendance. When training is mandatory and students are not paid for their attendance, the result will likely be a room full of unmotivated learners—not a great atmosphere for learning. Most likely there will be more sleeping and complaining going on during the sessions than learning.

---

[3] Shari M. Gallery (1990). Security Training Readings From Security Management Magazine. Boston, MA: Butterworths, pp. 93–113.

[4] Donald C. Mosley *et al.* (1993). Supervisor Management, The Art of Empowering & Developing People, Cincinnati, Ohio: South-Western Publishing Co., p. 354.

Scheduling should be done so that the learners are brought in for training after a rest period. That is, do not bring the student into a 4-hour class after the student has just worked 8 hours. Utilize the students' off days or evening hours if they work the day shift. Whatever you do, be sure to remember that in order to learn anything the student must be rested and motivated.

Technical colleges and community colleges can help alleviate scheduling and compensation problems. Your company can make it a policy for security officers to report to the local technical college within a certain time-frame, complete cognitive security officer training, and receive a certificate of completion. This would be made a condition of employment. You may even reimburse the officers for their training if they receive a certain grade which you set.

If the colleges only provide a pass/fail grade, then a certificate of successful completion could be used by the security officer to receive reimbursement. Since they must attend the college program on their own time, you can save the cost of paying their wages. There is one company that uses this initial training as a screening device. If you want to have a job you must complete a week or two of training and then compete for the job. Since the people being hired are not employees they receive no pay. After training there is no requirement that the person be hired.

Training the Trainer

Those who are designated trainers, as discussed above, must obtain credentials. The best way to attain teaching credentials is to attend the nearest technical or community college "Train-the-Trainer" course. This course is usually available at most colleges and universities. The fact that the training has nothing to do with security is irrelevant. Learning how to write a lesson plan, how to use different types of teaching methodologies and how to prepare tests are what you need for your credentials. You will add in security topics after receiving the basic training, when applying your knowledge in the classroom.

The trainer should also have some postsecondary or higher level credentials such as holding an AAS or BS degree in Security Management or some other degree in Security Management. Notice that we did not say a degree in Police Science, Criminology, or Public Law Enforcement. The reason for this is that there exists a great chasm between public law enforcement and private security. If you have never had a formal education in Private Security, then you may have a terrible time in court trying to prove to a jury that you were qualified to train security officers. Public law enforcement personnel have a very different attitude and perspective than private security practitioners.

In addition, the trainer should have at least 5 years' experience and a nationally recognized certification such as the Certified Protection Professional Certification (CPP) from the American Society for Industrial Security, a Certified Protection Officer (CPO) or Certified Security Supervisor (CSS) from the International Foundation for Protection Officers, or other such certification.

Imagine a situation where a lawsuit is filed and every one of your officers was trained at the local technical college. The instructor was a professional state licensed instructor who had 5 years of security management experience prior to becoming an instructor. The instructor had earned the CPP and CSS certifications in addition to his AAS degree in Security Management. Imagine also that each of your security officers has a training file which indicates that they all successfully passed the model curriculum set out above. These facts alone might make a litigious attorney hold off unless the facts of the case were rather lopsided in that lawyer's favor. In any event, negligent training would be very hard to prove.

Imagine the opposite. Let us say that all your security officers receive a few minutes of OJT in the way of training, with an experienced security officer. Compare the difference with the above scenario and determine which situation you would rather be in as a defense lawyer.

Evaluation of the Training Program and the Students

The best evaluation of the program is if it works. Are the security officers performing better? Has their public image and public relations improved? Do the officers seem to take more pride in their work and in themselves than they did before training? Do new recruits seem to reach productive levels faster? Has turnover slowed? Does the program curriculum seem

to match the practical application of job tasks? What comments do the officers make about their training experience?

Not only does the program need to be evaluated, but each officer should be evaluated to prove that he/she attained a certain level of knowledge. The training records should be kept in a file separate from personnel files. The cabinet should be of a bar and padlock variety with a secure lock. The files should contain such things as sample tests, student's answer sheets, their grades, and any comments made by the instructor. The student grade could be a number, a letter, or a P/F for pass or fail.

A separate file should be kept containing a copy of each revision of the training materials, including dates and times of each revision. A copy of all tests and a copy of the attendance sheet should be kept in this special file.

Testing for Learning Retention

The security supervisor may not be a certified classroom trainer, but he/she is clearly responsible for supervising on-the-job training for security officers under his/her supervision and for selecting formal training courses of value for them. The security supervisor is responsible for ensuring that these security officers attend formal training that is relevant, assures short-term learning from the classroom experience and provides long-term retention of that learning. That is, the training has to pertain to the job; the security officer should have learned something new and be able to display that learning after a suitable period of time.

Once the subject matter of the training has been selected (typically by corporate management or by the corporate training department), the security supervisor is in a position to recommend the local vendor or provider of the training. Since the subject matter has been predecided, the supervisor's choices are limited to the way in which the vendor guarantees that learning will take place and how long it will last. This discussion relates to one method for providing that assurance: an in-depth testing program.

In order to demonstrate that short-term learning has taken place, the individual must take a pretest and posttest on the subject matter and achieve more correct answers on the posttest than on the pretest. At the conclusion of the training, the security officer should be able to demonstrate sufficient short-term learning to indicate that the learning experience was worthwhile.

In order to demonstrate that long-term retention of the learning has taken place, the individual must take a posttest on the subject matter after a suitable period of time, say 6–12 months. More correct answers must be achieved than on the original pretest and almost as many correct answers as on the original posttest. The implication being that sufficient learning took place during the training experience to have become internalized and available to be built upon with further training.

The in-depth testing program described above is not typical of most training programs because of the additional cost involved. This does not mean that the testing concept should be abandoned; rather, it means that the security supervisor must demonstrate his/her ingenuity by establishing such a testing program on the job. Actually, this is not too difficult a chore for a good security supervisor who oversees an on-the-job training program.

Remember, the initial pre- and posttest are the same, but given at different times. The second or long-term posttest might be the same as the other two, but at this point the chance that the security officer will become "test-wise" or "test-sensitive" is too great. Rather, the security supervisor should consider an "observational" type of test. That is, the supervisor would have a checklist containing all the activities that the security officer should be performing that directly relate to the training received during the formal training and observe the extent to which those activities are actually being performed.

Development

Once the security officer is trained and put on the job, the officer should be given a calendar of required Continuing Education Units, CEU credits to be completed and noted by the

record-keeper before the end of the first year of employment. Each officer should be in class at least 6–12 hours or more in each 12-month period of employment. This training should not be restricted to cognitive classroom training, but could include hours spent at seminars, specialized OJT for the purpose of cross-training, recertification in first aid or CPR, self-defense training or college credit courses at a local accredited college.[5]

Nonetheless, the total hours must be calculated and a record kept in each officer's file. Any officer who fails to meet this requirement represents a breach in your legal liability coverage. A supervisor must be assertive in this area and insist on completion of continuous training from your security officer contingent.

Supervisors must also work to encourage the personal growth of their officers and ensure that their personnel are satisfied in their current positions. As a supervisor you are charged with the responsibility of evaluating your employees. You should attempt to motivate those under you and provide them with opportunities to achieve goals within the boundaries of your company. Therefore, development is not solely a matter of training, but also entails ensuring that each employee has the chance to move up or even move horizontally within the company. To accomplish this you must:

1. Analyze job descriptions and identify the skills in which each security officer excels. Find ways to expand the officer's areas of interest within the job description or suggest other similar job descriptions the officer might wish to explore.
2. Have the officer write down the objectives that he would like to reach and set a time line for their achievement. Discuss strategies on how these goals might be met.
3. If the security officer requires specialized training to reach the goals, find a way to allow the officer to attend the training.
4. Monitor and evaluate the officer's progress. If you find the officer backsliding, be quick to confront the officer with the behavior you observed and get the officer back on track.
5. Most of all, show sincerity and real concern for the future of each security officer. You must be a "can do" supervisor and prove it on a regular basis.

Conclusion

Training and development is not only concerned with meeting the needs of the trainee, but meeting the needs of the company as well. In the security industry, whether you operate a contract security business or serve as the proprietary force in a large company, the laws of the state, primarily the civil laws, dictate the training of security officers. Meeting these requirements helps security companies to avoid costly civil litigation. Of course there are other facets of law that must be considered, criminal law and administrative law for example, but most often it is with civil law that security departments become involved. Unfortunately, when a company becomes embroiled in a civil litigation over private security matters, the plaintiff too often wins. It is also true that under the tutored eye of a security expert conducting postmortems on these losses, most of them can be traced back to inadequate training or no training at all of the security officers.

Therefore, before you put this chapter down saying "yes, this all sounds nice, but we just cannot afford it," read page 1, paragraph 3 of this chapter, and ask just one question, "can we afford a $12.3 million dollar loss from a lawsuit right now?" The question is not whether you can afford security training, the question is whether you can afford to go without proper security training.

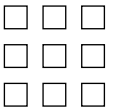
---

[5] Karen M. Hess and Henry M. Wrobleski (1988). Introduction to Private Security. 2nd edn, St. Paul, MN: West Publishing Co., p. 366

Staff Training and Development

Quiz

1. In order to properly protect your company from a charge of negligent training, it will be necessary to _____ the _____ before they are allowed to instruct.
2. There are three training domains. They are _____, _____ and _____.
3. _____ training consists of theory and knowledge portions of the training.
4. _____ training consists of the hands-on type of training.
5. _____ training consists of work values.
6. Training is a tool that can be used to avoid or mitigate legal problems brought on by the security officers. ☐ T ☐ F
7. One of the greatest mistakes made in the training of security personnel is failing to train the trainer. ☐ T ☐ F
8. "Adequate training" as defined by law, consists solely of showing security officers 6 hours of private security videotapes and having the officers fill out a 10-question test after each video. ☐ T ☐ F
9. Police officers who have never taken private security training and have never worked in private security are good choices to teach private security by virtue of their police training and years of police experience. ☐ T ☐ F
10. Trained security officers should be able to observe, report, and take limited action, in that order. ☐ T ☐ F



4 Curriculum Design

Daniel R. Baker

Introduction

Curriculum development and design requires the security training professional to understand, construct, implement, and evaluate required training curriculum on a recurring basis. This chapter provides a starting point for the security professional whose goal is understanding curriculum development and design. To meet that goal, there are 12 performance objectives to be mastered.

Performance Objectives

Upon completion of this chapter, you as a security supervisor will be able to:

- Define curriculum
- Distinguish between macro- and microcurriculum
- Select critical elements in the curriculum process
- Define competency-based education
- Identify the six-step process in determining competency-based outcomes
- Identify instructional goals
- Conduct instructional analysis
- Identify entry behavior characteristics
- Formulate performance objectives
- Develop criteria for writing performance-objective test items
- Implement an instructional strategy
- Select appropriate instructional materials

Your job as a security training supervisor is to ensure that each individual in your organization develops to the highest degree possible, all the requisite skills to succeed as a professional security officer. When you complete and master this material on curriculum and curriculum design, you should have the skills required to design, construct, implement, and evaluate a comprehensive security training program.

Why is it important that you as a supervisor understand and implement a credible security training program? The reduction of liability in security operations is directly related to the level of training provided to each officer. To ensure that the officer can do and does each task in the appropriate manner as required by policy and procedure is a training function. You are the most important cog in the wheel of security training. The manner in which you do your job in developing curriculum that supports organizational requirements can mean life or death to your security practitioners and ultimately to your organization.

This chapter is broken down into two parts: concepts in curriculum and curriculum design. In Part I, you will develop your skills in articulating and understanding curriculum in general, while in Part II, you will master the development and implementation of curriculum in security operations.

Part I: Concepts in Curriculum

Defining Curriculum and Distinguishing Between Macro- and Microcurriculums

Curriculum is normally defined as the sum of the learning activities and experiences that a learner has under the direction of a school or program. It is important to remember that in talking about curriculum you are discussing the sequence, continuity, scope, and balance of the materials which will be provided in a classroom or clinical setting. For the professional security curriculum, designer curriculum is best defined as a plan for learning that meets the needs of the organization, the security personnel to be trained, and the public served.

There are two types of curriculum that can be encountered in security training: micro and macro. Microcurriculum is the development of a task training step or unit of training within the confines of a larger course. Macrocurriculum is the development of a course or complete program of instruction that has multiple units or modules of study. This course is an example of a macrocurriculum because it is a complete course of study.

Critical Elements in the Curriculum Process

There are some critical elements that need to be considered when developing a curriculum. Do the training facilities support the desired educational outcome? Do the facilities have the requisite space, accoutrements, and rest areas necessary to support the students taught? These questions are directly impacted by your philosophy of education. Are you committed to the design and implementation of high-quality curriculum? Do you demonstrate your commitment to excellence in your approach to training policy?

A singularly critical element in the curriculum process, which we will discuss in greater length later, is the selection of students based on fair, consistent, relevant, and measurable standards—the "who is to be taught" issue.

The security curriculum design specialist must understand the importance of instructional media—the materials developed to support the curriculum that has been designed. Finally, the security supervisor responsible for the development of curriculum ensures that sound ethical principles, underlying tenets which are incorporated in the education process, are included in designed curriculum.

What then is the most important issue in the curriculum process? The developed curriculum itself—the plan for learning developed to assist the student in the educational process and those standards employed to ensure excellence.

Defining Competency-Based Education

Modern security education and training is competency based. There are a number of names currently associated with competency-based security training such as the following:

- Performance-based education or training
- Outcome-based education or training
- Behavior-stated education or training
- Criterion-referenced education and training

For the purpose of this course of study competency-based education is any educational process that requires the learner to demonstrate a skill, knowledge, or affective behavior based on a task, condition, and standard that specifies exact measurable outcomes. When speaking of performance, it becomes what the student can or will be able to do when trained. The behavior exhibited is the level of knowledge demonstrated, or skill displayed. Competency behaviors in curriculum design are broken down into four generalizable categories:

1. Unskilled: cannot do the performance
2. Semiskilled: requires close supervision

3. Skilled: can do most parts of the job or task with little supervision
4. Mastery skilled: can do all parts of the job or task, requires no supervision, and can teach others how to do the task or job.

Why should all curriculum designed by security professionals be competency based? The definition of competency-based training answers that question. Competency-based training is the process of setting clearly designed, measurable, observable objectives that the student learner accomplishes to a particular level. All competency-based training is designed around the development of objectives and the utilization of the developed objectives to measurable performance and/or accomplishment.

A competency is the knowledge, skills, and attitudes necessary to do a given task. Competency-based education and training for a security professional is an approach to learning where the student must demonstrate his/her ability to perform at a specific level prior to being certified as a Certified Protection Officer.

Six Steps in Determining Competency-Based Outcomes

What exactly do you need to get started writing competency-based security curriculum? You will need:

- A job description for each level of curriculum you intend to write. You use the job description to identify what the entry level, intermediate, or advanced security practitioner needs to know to accomplish the tasks described in the job description.
- A task analysis—you use the job description to complete a task analysis. A task analysis is the identification of the steps necessary to accomplish a specific part of the job being taught.
- A task sequencing—the analysis of each task from the standpoint of the untrained learner; simple to complex, known to unknown. The breakdown used by the trainer to identify the training sequence.
- Performance objectives for each task. An objective(s) based on task and task sequencing which tells the learner exactly what they must do, know, or complete.
- Measurement standards for performance that are objective and clearly identified so that misunderstanding does not occur.
- Developed curriculum that supports the performance objective specified for the competency task the learner is to be trained on. Curriculum that identifies the frequency with which the task will be accomplished or used, the importance of the task in doing the job, and the level of learning difficulty it will take to master the knowledge, skill, ability, or manner of accomplishment.

Part II: Curriculum Design

Each of us as security professionals wants to do a good job in training our subordinates. The difficulties faced sometimes seem insurmountable. This chapter will give you the tools necessary to increase your ability to incorporate sound system approaches into your curriculum design. Design construct, implement, and evaluate—those are the catchwords of a professional curriculum design specialist. The following materials will familiarize you with the Systems Approach Model for Designing Curriculum. It is one of many approaches to curriculum design. For the security supervisor designing curriculum, it is best because of its logical construction and ease of use.

Identify the Instructional Goal

The first step in the systems approach model for designing curriculum requires that you determine exactly what you want the students to be able to accomplish after the training is completed. This design step forces the designer to know exactly what must be taught. It also incorporates all the tasks within a duty to be viewed from the job as a whole. For example, the unit of instruction might be "Provide Entry Control" within a course entitled "Foundations of Security Practices." All of the tasks or units of training for the course come from a comprehensive job description.

In developing specific curriculum, the designer utilizes all of the learning domains: the cognitive domain for theory and general knowledge; psychomotor domain for demonstrated skills requiring use of the hands in performing tasks; and the affective domain for interpersonal, intropersonal or value-oriented skills.

The instructional goal may be derived from the following:

1. A listing of overall goals of the school, course, or unit of study
2. A needs' assessment—what really needs to be taught
3. From practical experience—the common sense approach to curriculum development
4. From analyzing how the job is already being accomplished

Conduct Instructional Analysis

The second step in the systems approach model for designing curriculum is conducting an instructional analysis. This is the process that occurs after you have identified the instructional goal and need to know what type of learning is required on the part of the student. It requires comprehensive analysis on the part of the curriculum designer to:

- Identify subordinate skills that must be learned.
- Determine subordinate procedural steps that must be followed to learn a particular process, skill, ability, or performance.
- Create a chart or diagram that depicts required skills and shows relationships among them.

Identify Entry Behavior Characteristics

Step three in the systems approach model for designing curriculum is determining entry behaviors and characteristics that will be required of those participating in the training program. Every course of instruction has a minimum level of competency which must be met. For security, it is normal to require the applicant to be at least 18-years old, have no history of alcohol or drug abuse, and have no felony convictions. These are all entry-level behaviors or characteristics required for employment. But more than these, security applicants should be able to read and write, exercise sound judgement, communicate effectively, and demonstrate the ability to control outbursts of temper under stress. These entry-level behaviors and characteristics are normally:

- Required for entrance in the training program
- Required for successful completion of the training program
- Required by policy or practice

Entry behaviors and characteristics are not simply a listing of what the student can do, but specify what is required of the student to participate in the learning process. These required behaviors and characteristics identify any specific characteristic of the learner that may be important to consider in the design of specific curriculum.

Step four in the systems approach model for designing curriculum is writing the performance objectives. Written performance objectives are based on the instructional analysis. They incorporate specific entry behaviors and characteristics, and are specific statements of what the learner will be able to do upon completion of the course of study, unit of instruction, or task training. All written performance objectives:

- Identify knowledge, abilities, or skills to be learned and the task to be accomplished.
- Identify conditions under which the knowledge, ability, or skill must be performed, and what will be provided to the student to complete the action required.
- Identify criteria (standards) for successful performance.

One example of a written performance objective would be:

"Upon completion of this chapter each security supervisor participating will (provide pencil, paper, and a desk) write one performance objective for a psychomotor task to the satisfaction of the test examiner."

The performance objective has a clear statement of the knowledge, ability, or skill that has to be mastered: "write one performance objective." It has two clearly stated conditions: "Upon completion of this course of study" and "provided pencil, paper, and a desk." Finally, it has a measurement statement: "to the satisfaction of the test examiner." The standard for successful performance could be without error, to a score of 85%, list 6 out of 10 approaches to curriculum design. It simply must have a statement that the students can utilize to know exactly how they will be evaluated.

Develop Performance Objective Test Criteria

The fifth step in the systems approach model for designing curriculum is the development of the performance-referenced test. The performance-referenced test is based only on the performance objectives specified in the development of curriculum. To that end, the performance-referenced test is written before the lesson plans or reference materials to be used in the course of study or training program. It is the formal evaluation instrument that will be used to measure the learners' accomplishment of the specified requirements for successful completion of the competency.

If the performance objective says the learner will write, the performance test question would require writing. Using the performance objective written in step four above, the test question would be a statement: "Write a performance objective for a psychomotor skill." The directions for the accomplishment of this test item might be: Provided a pencil, paper, a desk, and time to accomplish the task, each student will write a performance objective for a psychomotor skill to the test examiner's satisfaction.

The test examiner then must be a subject content expert in the construction and evaluation of performance objectives. Why? The measurement standard should be objective and not subjective. Subjective answers are graded only by expert examiners because they require consistency in the standard used to measure accomplishment. In completing the performance objective test task, the student would simply have to ensure his/her answer including:

- Statement of the knowledge, abilities, or skills to be accomplished
- Condition(s) under which the knowledge, abilities, or skills must be performed and what will be provided to the student to complete the action required
- Measurable standard for identifying successful performance

Implement an Instructional Strategy

In the sixth step of the systems approach model for designing curriculum, the curriculum developer finally starts to make choices on the instructional style or strategy that will be used to facilitate learning. There are four primary strategies that can be used in curriculum development.

- Instructor-centered learning. The instructor provides all the information to the student and evaluates performance. The difficulty of this method is that it is personnel intensive, normally occurs in a lockstep model, every learner learns at the same rate, and does not account for learner differences. The instructor-centered approach is normally lecture oriented.
- Individual-centered learning. A plan is developed between the learner and the instructor (supervisor) on what is to be learned, how long the student will take to accomplish the learning, to what level the learning will be measured, and how. This method is chosen when the individual is success oriented, demonstrates a high degree of discipline, and requires low structure in the learning environment. The individual-centered approach works best with individuals studying for advanced outcomes.
- Interactively centered learning: A process for developing critical skills. The learner interacts with the environment by verbalizing learning, participating in discussion groups, or demonstrating competencies. This method of curriculum design requires a high degree of motivation on the part of the learner and incorporates case studies,

panel discussions, and real-time demonstrations in the learning activities. Interactive learning is the hands on approach to skill mastery.

- Experiential-centered learning: A process that incorporates cognitive, psychomotor, and affective learning in field or clinical settings. The experiential approach places the student on the job while at the same time requiring ancillary learning by study, drill and practice, and evaluation. Experiential learning is considered the best type of learning because it marries theory with practice.

In determining the instruction style or strategy to be used in the development of curriculum, the security training professional utilizes each previous part of the systems approach model for curriculum design. They also develop a timetable for all preinstructional activities that must be accomplished. Select the method or methods in which the material to be mastered wilal be presented. Determine how student feedback will be gathered. Designate the methods to be used in testing and identify testing material needs. They also implement a strategy for follow-through activities to ensure the curriculum is designed, developed, constructed, and implemented as planned.

The security training director ensures that all curriculum is based on current research in learning theory, utilizes the best current knowledge available on learning as a process, and clearly, concisely, competently, and correctly specifies the content to be taught. The single constraint placed upon the design of the formal curriculum is the mandatory characteristics or behaviors required of the learner to participate in the process.

Select Appropriate Instructional Materials

The final step in the formal construction of security or public safety curriculum is the development and selection of instructional materials. The security training profession provides the learner with a training manual. The manual provides written guidance for successful course completion. It provides the learner with the competency outcomes they will have to master to satisfactorily complete the program of learning and specifies the evaluation process.

Just as the learner is provided a manual, the instructor is also provided with all training materials. The instructor is provided with all the competencies to be taught, lesson plans, student activities sheets, demonstration performance materials, transparency masters, equipment, and any other educational materials necessary to conduct the training. Perhaps the most critical teaching tool given to the instructor is the instructor guide. The instructor guide places the unit, course, or performance in context with the educational goal. It is the road map used by the instructor to teach the sequenced lessons or facilitate the learners' study.

Testing materials are selected from a created test bank that holds a number of questions written for specific performance objectives. Every performance objective written for the course is tested. If the material does not need testing, a performance objective should not have been written. There are two types of tests. Every unit of instruction should have both of these tests. Validation of learning occurs in the measurement of educational gains between the pretest, instruction or study, and the posttest. If the student demonstrates on the pretest that they already know the material to a specific standard set in the performance objectives, they should be allowed to move to the next unit without participating in the individual instructional or study unit.

You as the security training supervisor, director, or training officer will have to decide if you want to develop new material for your training program. This course and all the work that went into it represents a large investment on the part of the International Foundation for Protection Officers. They made their decision based on a recognition that suitable materials were not available to meet your needs. Remember it is always cheaper to adapt current material than it is to design new curriculum. Another idea is to adopt material that was written for another organization if it is possible and it meets your needs.

In concluding this section on the selection of curriculum remember the four specific questions you should ask:

- What is the cost of designing new materials?
- What materials currently exist that might meet our needs?
- Do the materials that exist support our performance objectives?
- What other organizational criteria need to be considered in the existing material?

Conclusion

After you have completed designing your curriculum you are not through. The final stage in developing curriculum is the evaluation process. Again there are two types of evaluations you should conduct, formative and normative. Formative evaluations are conducted prior to testing the curriculum. The first normative evaluation provides a baseline for further comparisons with follow-up on students or classes. These evaluations are conducted constantly to ensure the curriculum is accomplishing its goal or goals and to keep it current.

Formative evaluation is initiated upon completion of draft instructional materials. It may be accomplished in one of three ways: in one-to-one consultation with another subject content training expert; subjected to evaluation by a small group of training professionals who specialize in the curriculum designed; or in some cases the formative evaluation is conducted in field evaluations if the material is time critical or sensitive. The formative evaluation process may be used for a course, unit of instruction, classroom lecture, or demonstration performance.

Normative evaluation is based on some level of acceptable standard. How many days, hours, or questions may be missed and still pass or complete the course? Should the student be able to accomplish the task with no supervision, some supervision, or while closely supervised? What are the accepted tolerances? Must the task be accomplished without error, or as indicated, in some other manner?

Normative evaluations should be objective and not subjective. When dealing with theory or cognitive material there should be a written test. The demonstration of a skill requires application in a real work scenario and effective skills are evaluated when the learner models acceptable behaviors.

Both formative and normative evaluation are the first steps in redesigning curriculum in the systems approach for designing curriculum. They identify difficulties experienced by the learner, based on the successful or unsuccessful accomplishment of performance objectives. Formative and normative evaluations identify deficiencies in instruction.

They ultimately attest to the worth of the curriculum design and are used to validate the effect, efficiency, and cost-effectiveness of the educational process. Formative evaluations are conducted best when someone outside the organization reviews all the material to measure suitability and the accomplishment of stated competency goals. Finally both evaluations are based on quality not quantity.

Summary

The completion of this unit has provided you with the information you will need to: define curriculum, distinguish between micro- and macrocurriculum, select critical elements in the curriculum process, define competency-based education, identify the six steps to determine competency-based outcomes, identify instructional goals, conduct an instructional analysis, and identify requisite entry-level behaviors and characteristics for entrance into the learning program. You have also learned how to formulate performance objectives, develop the criteria for writing performance objective tests, implement, and identify an instructional strategy and select appropriate instructional materials.

With these skills you will be able to construct a comprehensive, performance-oriented training program. The use of the systems approach model for the design curriculum focuses the security training professional on the task at hand: training today's security officers for tomorrow's challenges.

Curriculum Design

Quiz

1. Curriculum development and _____ requires the security training professional to understand, construct, implement and evaluate required training curriculum on a recurring basis.

2. Modern security education and training is _____ based.

3. The first step in the systems approach _____ for designing curriculum requires that you determine exactly what you want the students to be able to accomplish after training is completed.

4. The final step in the formal construction of security or public safety _____ is the development and selection of instructional material.

5. With these skills you will be able to construct a comprehensive, _____ orientated training program.

6. Curriculum is best defined as a plan for learning that meets the needs of the organization, the security personnel to be trained, and the public served. ☐ T ☐ F

7. Microcurriculum is the development of a task training step or unit of training within the confines of a larger course. Macrocurriculum is the development of a course or complete program of instruction that has multiple units or modules of study. ☐ T ☐ F

8. A singularly critical element in the curriculum process is the selection of participating learners based on fair, consistent, relevant, and measurable standards—the "who is to be taught" issue. ☐ T ☐ F

9. Competency-based training is the process of setting clearly designed, measurable, observable objectives that the student learner accomplishes to a particular known level. ☐ T ☐ F

10. A job description is not needed when determining competency-based outcomes ☐ T ☐ F

5

Professional Certifications: Milestones of Professionalism

Inge Sebyan Black and Christopher A. Hertig

Professional certification programs are established within each industry. The security industry has a wide array of professional certifications and we will try to address and highlight some of them. Before the certification programs themselves are discussed; it is necessary to lay a foundation regarding what constitutes a "profession" and what a "professional" is.

Members of a profession are regarded as professionals. Professions generally have the following components:

1. A recognized body of knowledge. This body of knowledge is unique to the profession. In security this would primarily be physical security. It can also include supportive knowledge shared with other fields. Medicine uses biology and chemistry. Security encompasses a myriad of other disciplines from psychology and sociology to physics and law. Security also interfaces with management, policing, and safety. Increasingly, there is a stronger bond being forged with emergency management.
2. Advanced education and training. This is an extensive learning regimen undertaken only by members of the profession. It uses both theoretical and applied knowledge. This has taken some traditional educational forms in the past such as with law school, medical school, or the seminary. Emerging professions such as policing and security will utilize a more diverse array of means to develop knowledge, skill, and ability. Much of this will focus upon maintaining currency in one's field. These learning experiences will include distance education, seminars, licensing, and various types of certification processes. The latter will include user certifications such as becoming accredited by a manufacturer or provider in the application of some particular system (Management of Aggressive Behavior, Nonviolent Crisis Interventrion, the Reid or Wicklander-Zulawski interviewing method, etc.). Instructor certifications can also be included in this category. Of particular importance are professional certification processes awarded by nonprofit professional organizations.
3. An experiential component or apprenticeship of some sort. This can be an internship, apprenticeship, or required amount of time spent in the practice of the profession.
4. Adherence to a code of ethics. Members of profession share a consensus on what encompasses ethical conduct.
5. A professional organization or association. This professional association facilitates the exchange of new research, legal standards, and methods of operation. It also creates and enforces ethical standards among members. Professional associations represent the profession to the public via lobbying efforts, news releases, websites, etc. The results of studies and research are also proffered to the public so that the public sees

the organizatio as an authoritative voice for the profession. In medicine there is the American Medical Association; in security we have American Society for Industrial Security (ASIS) international. The future of the security profession is intimately tied in with both research and various means of public outreach.

6. A degree of exclusivity which prevents anyone and everyone from laying claim to eing a member. This takes many forms from rigorous educational and training standards to association membership, extensive apprenticeships, and in some cases government regulation.
7. Recognition by the public that it is a profession. Rigor, research, and exclusivity all help form the "product" that is marketed to the public. Public relations efforts married with the passage of time help the profession gain acceptance.

The Individual Professional

Professionals are those individuals who are members of a profession. They practice the profession through their employers or clients. Professionals study and practice a variety of methods in the pursuit of perfection. They are committed to the profession and have a special relationship with their employers and clients. Professionals have undertaken advanced study within their area and hold advanced academic degrees, professional certifications, or both.

Virtually every industry has professional certifications, specific for that industry. Their utility is increasingly important in an international economy. It may well be argued that in the United States we are slow to adapt professional certifications; that "letters after one's name" have been more widespread in other countries throughout the world. Professional certification processes are important for recognition by one's peers, employers, clients, and students. Professional certifications are career milestones which are represented by the holder using the designation after their name. Examining the purpose of any certification program reveals that these programs/processes exist for the following reasons:

- To elevate the visibility of the specific profession. Professional certifications do this, in part, by enabling the holder to place the initials after their name. Another method of visibility enhancement is through the media relations of the certifying organization.
- To encourage and mandate continued professional development, education, and technical skills. Most professional certification programs require some type of continued professional development. This may consist of taking classes, attending conferences, maintaining membership, and speaking or writing about the professional body of knowledge.
- To ensure minimal criteria of the knowledge, skills, and abilities of the profession. Professional certification programs do this by requiring a specified amount of experience, education, and training in some combination.

Benefits of Professional Certification to Society

Society at large benefits from professional certification processes in security. Security professionals who are certified receive recognition of that. Clients, employers, and end users of the professional's services (customers, visitors, tenants, etc.) see the certification and know that the holder meets a higher standard of expertise than someone without it. This is an important point as the public at large is increasingly dependent upon security professionals for their protection. More and more mass private properties such as shopping centres and office complexes are frequented by the public and protected by independent security forces. These forces may be proprietary, contract, public, or private. They are led and managed by security managers; all of whom can better perform their diverse and challenging functions if they have gone through a rigorous certification process.

In another vein is state and provincial licensing of consultants, investigators, security officers, and others. Professional certification can play a key role here. As the certification processes are almost invariably administered by a nonprofit organization; the government

regulatory agency can easily incorporate them. This ensures quality service at low cost as the state agencies do not have to develop programs; they can simply adopt those already in place. If licensed private investigators were required to be either Certified Fraud Examiners or Professional Certified Investigators the licensees would meet a higher standard. Regulations could easily be adopted to require that principals in security service firms hold the Certified Protection Professional designation. Similarly, certain supervisory personnel could be mandated to hold the Certified in Security Supervision and Management credential. This may be appropriate for persons who hold a license or oversee a certain number of persons. The Certified Protection Officer Instructor process would be an ideal requirement for those state or provincial certified training instructors who teach security officers.

Benefits of Professional Certification to Employers, Clients, or Students

Employers, clients, and students or certified individuals benefit in many ways. Employers of professionally certified individuals benefit by having their personnel earn a recognized benchmark credential. This can easily be incorporated into a vertical or horizontal promotional scheme. It can also be marketed externally through press releases to general news media as well as industry-specific publications.

Clients of designated persons receive a substantial degree of assurance of professional competence. In some cases, having security service firm employees complete professional certification processes is an excellent means of quality assurance that can be written into a contract. In other settings the client firms can assess how much contract companies support professional certification. Those that only give it lip service or have a token designated individual on staff are best avoided. Leading security service firms understand the importance of professionalism and embrace certification processes. Securitas and G 4 Security Services (formerly Group 4Falck) have both embraced professional certification in a meaningful way. Both firms have demonstrated their commitment to excellence by promoting certification of their personnel.

Students in particular benefit as professional certification in security provides a major part of the answer to teaching qualifications. As there are few doctoral programs in security, the most expedient means of obtaining relevant teaching credentials for doctorate holders in other related disciplines is to become professionally certified. A PhD in sociology who had worked in security could become a Certified Protection Officer. A PhD in management who had been an accountant could become a Certified Fraud Examiner. The International Foundation for Protection Officers offers scholarships to faculty for this very purpose. In addition, The Certified Protection Officer Instructor designation is ideally suited for those who teach; be it in an academy, secondary school, college, or university.

Benefits of Professional Certification to the Individual

A professional is said to possess a large degree of knowledge derived from extensive academic and practical training. The level of academic and practical training sets individuals apart through one, several, or all of these: training, testing, education, and experience. Many require recertification to maintain a higher skill level and to keep up with changing times.

Since security is almost synonymous with trust, certification makes an impact. Being a professional means one is likely acting through established protocols for licensing, ethics, procedures, standards of service, and training/certification. Those who strive to be a professional, do so by being self-regulating, in that they control the training and evaluation process. Being certified also states that besides having education and skills, they are also mature, have learned lessons and provided benchmarking. Professional certification can bring one growth, recognition, promotion, and opportunities. Professionals are expected to utilize their independent judgement that they have learned through study and practice. While professional development is recommended for every security professional, it is imperative that those of us in the supervisory role make lifelong learning a critical part of our responsibility.

Professional development often refers to skills required for maintaining a specific career path, or to general skills offered through continuing education. It might include general skills in the area of personal development or it might be training to keep current with changing technology and practices in security, otherwise known as lifelong learning.

"Security" is a very broad and all-encompassing term. One's position may require the provision of executive protection services, protection against liability, protection of intangible or tangible assets, prevention of fraud and embezzlement, information protection emergency management, and so on. Few security positions include every one of these but most include several. The specific certification obtained will depend on the responsibilities and skills the holder wants or needs to learn. By finding mentors, joining a variety of security organizations, and subscribing to security publications, one will be able to determine which certification best fits them and their organization. Taking time to become certified validates one's professional development and shows a commitment to self-improvement and adherence to increasingly high standards within the security industry. Certification also provides opportunities for personal growth and brings well-deserved recognition from peers and colleagues.

Professional certification is much like higher education; except that there is an experience requirement and usually a recertification mandate. It is like higher education in that it broadens the individual. It helps prepare them to take on additional responsibilities. While not expert in everything covered in the certification exam; the holder at least has a working knowledge of it. From there he/she can learn more. Like a college degree holder who can learn more quickly than someone without a degree; the professionally certified individual has a "head start" on professional development. They can adapt more readily to career challenges.

Being professionally certified offers one an immense degree of personal accomplishment that is impossible to put a price on. Having the letters after one's name is very gratifying. It is also more likely to grab the attention of prospective employers and clients. Individuals who do not know what the letters mean will ask. Those that desire some degree of benchmarking will require them.

Aside from the obvious advantage a certified individual has in competing for jobs and clients against those that do not; there is also the issue of career longevity. Getting a job or client is not as important as keeping one. Being professionally certified means being professionally connected. Having access to information and colleagues aids one tremendously throughout their career.

The Responsibility of Being a Leader in Security

Those who have risen to the level of supervision or management in security are most likely respected, trusted, and treated as professionals. Their experience level is above that of others and along the way they have developed skills that are quite substantial. Development is an individual process. One must be dedicated to learning and willing to sometimes learn an entirely new way of doing an old job. The responsibility we have is to advance our skill level so that we can appropriately help to develop those who work for us. The obvious implication is to lead by example: supervisors and managers should seek out the appropriate professional certifications. They must then inspire their subordinates to do likewise.

Professional Security Organizations

Membership in a professional security organization allows us to associate with like-minded individuals. Through mentoring and being mentored, we learn new skills, gain new insight, fresh perspectives and that keeps us current in our field. Being a part of a security organization allows members to gain access to a variety of professional certification programs and a large array of training programs. There is a relatively large choice of such organizations. The following discussion contains highlights of a few of the more prominent professional organizations. The list below is by no means all inclusive; additional processes are bound to evolve. The current efforts being undertaken by the Retail Industry Leaders Association appear to be quite laudable. The development of a designation for entry-level retail loss prevention personnel (LPCQualified) who then acquire the requisite education and experience

can take an exam to become LPC Certified is exciting (http://www.lossprevention certification.com/accessed January 26, 2007).

There is, however, a caveat that must be offered at this point. That is to always ascertain the credibility and longevity of the designation and the organization awarding it. One of the authors was accredited as a PsychoMotor Skill Design Instructor (PSDI) by an organization that has since become defunct! One does also not want to be in the position of having to defend his/her credentials from the demeaning remarks of colleagues, clients, and courts!

Below are listed some of the major certifying entities. Descriptions of the certification processes follow; however, it is important to remember that these change and one must always review the current requirements.

1. The International Foundation for Protection Officers (IFPO)

IFPO was established in 1988 for the purpose of facilitating the training and certification needs of protection officers and security supervisors from both the commercial and proprietary sectors. Associate (nonvoting) membership is available to any person who is employed in security. Each application for membership must be supported by including, as references, the name and address of two security professionals. Members receive a certificate of membership, identification card, lapel pin, membership directory, Protection Officer News (quarterly newsletter), and enjoy a 10% discount on IFPO-sponsored programs. Corporate memberships are also available. A variety of security publications addressing important topics within the security industry can be obtained at a very modest cost. Topics include crime prevention programs, civil liability for security personnel, protection officer survival, special events planning, careers in security and investigation, and high-rise building security. IFPO offers two security certification programs: the Certified Protection Officer (CPO) and the Certified Security Supervision and Management (CSSM) programs.

The CPO program is open to all security officers. The program is designed for protection professionals whose intent is to improve their individual security skills. They should also be comfortable with a self-paced, home-study style of learning. To earn the CPO designation, candidates must study the Protection Officer Training Manual and successfully complete an unsupervised mid-term examination and a proctored final examination. The CPO program covers an array of security topics including physical security, investigations, fire prevention, crime scenes, emergency procedures, bomb threats, report writing, and crisis intervention. The curriculum exceeds the recommendations of many governmental and professional organizations in terms of scope. Membership in IFPO is not required for enrolment in the CPO program but Foundation members receive substantial discounts.

The IFPO also sponsors a Certified Protection Officer Instructor (CPOI) designation which is oriented toward teaching and mentoring CPOs. CPOIs must first be Certified Protection Officers. They must also possess education above the secondary level and have experience both in teaching and in security. In addition they must be certified to instruct in one or more subjects by a professional, military or governmental organization. There are over 500of Certified Protection Officer Instructors throughout North America, Europe, and the Middle East.

The Certified in Security Supervision and Management (CSSM) program consists of a two-part process. First, the candidate must complete the Security Supervision and Management program. This distance-learning course is designed to meet the needs of the security supervisor or senior protection officer. It is also easily adaptable to undergraduate and graduate college programs.

The second step for the candidate who has successfully completed the Security Supervision and Management program and wishes to become certified, is to possess the required amount of security industry experience. Eighteen months of full-time protection experience with at least 6 months in a supervisory role is required. Part-time experience is acceptable on a 2 for 1 ratio. The next step is for the candidate to complete a series of simulated workplace scenarios demanding supervisory action. Candidates must describe the measures they deem appropriate for each scenario and substantiate the recommended actions by using the course text (*Security Supervision: Theory and Practice of Asset Protection*) as supportive reference.

Ph. +1 877/247-5984

http://www.ifpo.org/

2. ASIS International (ASIS)

ASIS was founded in 1955 as the American Society for Industrial Security. It is one of the premier organizations in the security industry. Its purpose is to promote and establish professionalism in the field of security. Membership in ASIS is strictly individual; corporate memberships are not available. New members are required to complete an application, which must be endorsed by a Chapter Officer or Regional Vice President. The prospective member must also be sponsored by an ASIS member in good standing. Membership is open to all security professionals who are currently employed in a position with responsibility for the security function of a business, institution, or government agency in a position of responsible charge. ASIS defines responsible charge to mean "that charge exercised by an individual who makes decisions for the successful completion of objectives without reliance upon directions from a supervisor as to the specific methods or techniques."

ASIS members receive Security Management, a leading professional magazine. Also included in membership is the Security Industry Buyers Guide. This guide is a very handy resource for locating security services. Of even greater utility for locating colleagues worldwide is the membership directory which is published in both a print and web version. The Directory lists members by name, organization, and location so that making contacts is facilitated. Within ASIS, there are many ways to network and gain professional development. Some are through ASIS local chapters, of which there are more than 200 worldwide. ASIS provides a host of educational programs including training at the Annual Seminars & Exhibits. Student members of ASIS receive all the benefits of regular members at a fraction of the cost.

ASIS also sponsors the Certified Protection Professional (CPP) program. The CPP program was initiated in 1977 and is the premier certification for security managers. Over 10,000 individuals have been certified around the world and the CPP is mentioned in a substantial number of job announcements for security managers. The designation is also recognized by several governmental entities.

To be eligible to sit for the CPP exam, the applicant must meet the following standards:

- Nine years' experience, at least three of which were in a position of responsible charge, or
- A Bachelor's degree from a regionally accredited college and 7 years of experience, at least three in a position of responsible charge.

Each applicant must be endorsed by a CPP in good standing and must affirm adherence to the ASIS code of ethics. The applicant must successfully complete a written exam and recertify every 3 years.

The Physical Security Professional (PSP) designation was introduced in 2002. It is a technical designation focusing upon physical security design and requires in-depth knowledge of installation, operation, and integration of physical protection systems. Candidates must have a minimum of 5 years experience.

The Professional Certified Investigator (PCI) is for those having 5 years or more of investigative experience with at least 2 years in case management. The PCI certification may give one a competitive edge in the complex business of investigation.

ASIS International
Membership Department, Suite 1200
1625 Prince Street
Alexandria, VA 22314
United States
Ph. +1 (703) 519-6200
http://www.asisonline.org/

3. The Association of Certified Fraud Examiners

The Association of Certified Fraud Examiners (ACFE) was founded as a professional organization for fraud examiners. Its mission is to reduce the incidence of fraud and white-collar

crime and to assist the membership in its detection and deterrence. There are different types of membership categories.

- Associate membership is open to anyone interested in the prevention, detection, deterrence, and investigation of fraud and fraud-related activities.
- Regular membership is open to current members of the ACFE. The Certified Fraud Examiners (CFE) is a globally preferred credential that is a symbol of quality in the antifraud profession.
- Educator Associate is available to those who are employed by an institution of higher learning, as an educator, as your primary means of employment.
- Student Associate is for those undergraduate students enrolled at least 12 semester hours or a graduate student enrolled at least 9 semester hours, in a college or university.

Members have immediate access to ACFE publications, continuing education opportunities, networking opportunities, and professional growth. The association sponsors the CFE designation. This certification denotes proven expertise in fraud prevention, detection, deterrence, and investigation. Members with the CFE credential experience professional growth and quickly position themselves as leaders in the global antifraud community. Generally, applicants for CFE certification have a minimum of a Bachelor's degree (or equivalent) from an institution of higher learning. No specific field of study is required. Those without a Bachelor's degree may substitute 2 years of fraud-related professional experience for each year of academic study. At the time of certification, the candidate must have at least 2 years of professional experience in a field either directly or indirectly related to the detection or deterrence of fraud.
Association of Certified Fraud Examiners
716 West Avenue
Austin, TX 78701
United States
Ph.: +1 (800) 245-3321 (United States and Canada only) or +1-512-478-9000
http://www.acfe.com/

4. The International Information Systems Security Certification Consortium or (ISC)2®

ISC2 is internationally recognized for educating and certifying information security professionals throughout their careers. They have over 42,000 information security professionals in more than 110 countries. Founded in 1989 by industry leaders (ISC)^2 issues the Certified Information Systems Security Professional (CISSP®) and related concentrations: Information Systems Security Architecture Professional (ISSAP®), Information Systems Security Management Professional (ISSMP®) and Information Systems Security Engineering Professional (ISSEP®); the Certification and Accreditation Professional (CAP^{CM}); and the Systems Security Certified Practitioner (SSCP®) credentials to those meeting the necessary competency requirements. Several of (ISC)^2's credentials meet the stringent requirements of ANSI/ISO/IEC Standard 17024, a global benchmark for assessing and certifying personnel. (ISC)^2 also offers a portfolio of education products and services based upon (ISC)^2's CBK®, a compendium of industry best practices for information security professionals, and is responsible for the annual (ISC)^2 Global Information Security Workforce Study.

Membership is open to professionals who have as their primary responsibility information systems security, educators, students, attorneys, and law enforcement officers having a vested interest in information and data security; or professionals with a primary responsibility for marketing or supplying information security products or services. ISSA also provides a professional certification, Certified Information System Security Professional (CISSP). Requirements for the CISSP designation include experience and/or the successful completion of an examination. The CISSP credential is ideal for mid- and senior-level managers who are working toward or have already attained positions as CISOs, CSOs or Senior Security Engineers. The CISSP program consists of coursework in access control, application security, business continuity and disaster recovery planning, cryptography, information security

and risk management, legal, regulations, compliance and investigation, operations security, physical (environmental) security, security architecture and design, telecommunications and network security. The CISSP I is the first credential accredited by ANSI to ISO Standard 17024:2003 in the field of information security.

ISC² Institute
1964 Gallows Road
Suite 210
Vienna, VA 22182
United States
Ph: +1 866-462-4777 or +1 703-891-6781
Fax: +1-703-356-7977

5. The International Association for Healthcare Security and Safety

The International Association for Healthcare Security and Safety (IAHSS) was founded in 1968 for hospital security and safety administrators. Today IAHSS embraces the entire health care industry and has grown to be the largest association of its kind. Membership is open to individuals who are active in the field of hospital/health care security and safety. Members receive the Journal of Healthcare Protection Management, the IAHSS Newsletter and membership directory. IAHSS offers numerous training programs, including the Security Officer Basic Training Certification Standard (40 hours), Supervisory Development Standard (20 hours) and the Safety Training Standard (20 hours). IAHSS also offers the professional designation, Certified Healthcare Protection Administrator (CHPA) to qualified members. Becoming a CHPA is a two-part process.

First, the candidate must be accepted at the nominee level. To achieve nominee status, the applicant must be, or must have been, the security/safety risk management/manager of a health care facility. The applicant must submit a completed application clearly documenting the accumulation of 10 credits among 4 categories of education, experience, membership, and specialized training. Credits are awarded in each category based on the degree of education, number of years of experience, number of years as a member, and the number of specialized training courses completed. Second, the nominee must successfully pass a written examination covering four bodies of knowledge (management, security, safety/life safety, and risk management).

P.O. Box 637
Lombard, IL 60148
United States
Ph: +1 (630) 953-0990
http://www.iahss.org/

6. The International Association of Emergency Managers (IAEM) (http://www.iaem.com/)

The International Association of Emergency Managers has both the Associate Emergency Manager and Certified Emergency Manager (CEM) programs. Certified Emergency Managers must have 3 years of comprehensive emergency management experience supported by references (including the candidate's current supervisor). A baccalaureate degree is required; additional experience may be substituted at the rate of 2 years experience for every 30 credits. The Associate Emergency Manager (AEM) is available for individuals who meet all CEM requirements but do not have college credits.

- One hundred contact hours of emergency management training and an additional 100 hours of general management training are required.
- Contributions to the profession are required. Six separate contributions beyond the scope of job requirements are required. These include professional membership, speaking, publishing articles, serving on boards, or committees, etc.
- Examinations include an initial 100 question multiple-choice examination and a comprehensive emergency management essay.

These are a few of the many different organizations that can help develop individuals as professionals. Each one focuses on different areas of knowledge, skill, and ability. Each one aids its members in different ways. All of them help to pave the way for professional advancement.

Many organizations will have in-house training programs. In-house training allows companies to keep down costs and maximize training time. Most employers, however, are not large enough to provide all the training necessary to accomplish their mission. This is especially true of security training, and the more specialized it is, the more difficult it is to provide in house. For this reason alone, serious thought must be given to external training resources. An additional consideration for the individual is career advancement: in-house programs do not carry nearly the degree of recognition that professional certification processes do.

Proprietary programs, college programs, and professional certifications all have their place in the development of protection professionals. In-house programs can supply components of knowledge that may be part of professional certification programs. One trend that shows tremendous promise is for organizations to run training academies which teach the Certified Protection Officer curriculum. Contract security service firms do this and use it as a developmental and recruitment tool. Having an academy also adds to the prestige of an organization in the eyes of both internal and external customers.

Another way to seek further development is college courses, whether it is for credit or noncredit. Regular academic classes can focus on topics that are included in certification processes such as Investigation, Emergency Management, Terrorism, etc. They can also utilize texts for professional certifications as part of their courses. Such an approach gives value-added to students who can use the text for multiple purposes: the college course, preparing for the certification, and as a reference. This is no small issue in the online age where students buy texts less and, perhaps, read them less. At York College of Pennsylvania, the Certified Protection Officer Program, the Security Supervision and Management Program and the Crime and Loss Investigation Programs are largely covered within existing courses. Regular college courses use the texts for the various IFPO Programs. As an example, CJA102 Introduction to Security and Asset Protection and CJA305 Criminal Investigation each cover approximately one third to one half of the Crime and Loss Investigation Program. This enables students to complete the Crime and Loss Investigation Program on their own.

An increasing number of secondary schools which offer Protective Services curricula incorporate the CPO as a final exam. While the CPO is at a level above that of typical high school students, it can be incorporated into a curriculum rather easily. The CPO is broken into parts over the course of several years and is given as a final examination. The students gain the required experience by patrolling the school campus, monitoring central stations, and in some cases doing externships or "shadowing" with local security departments. The schools gain a ready means of outcomes assessment.

Colleges may wish to incorporate IFPO programs into their curricula as a value-added service to students. Using Foundation texts and online support can help expand an existing curriculum in terms of both content and time: students have more available to them than the instructor has prepared. They also have material that they can study after the college course is over. A motivated individual can continue their study and receive a certificate such as the Crime and Loss Investigation or Security Supervision and Management program. They can then continue on with additional study and experience and attain the Certified Fraud Examination, Professional Certified Investigator or Certified in Security Supervision and Management credential.

Colleges with certificate programs or academic minors in Security may take a similar approach. An added benefit to this approach for colleges is that it may be the ideal way for them to integrate distance education with traditional classroom instruction. This is likely to become a very prominent issue within higher education in the coming decade. Increased competition and the eventual entry of online degree programs for the traditional college student will change the educational landscape. Only those institutions that wisely develop their curricula, integrating traditional and online instruction, are likely to succeed over time.

Preparing for professional certifications is an incremental process. Professional certifications take time. One becomes designated after acquiring the knowledge and experience. Persons should not become intimidated by the extensive experience requirements mandated

in certain programs. The appropriate perspective is to view this as a journey. Remember the old adage:

"The longest journey begins with the first step."

Candidates should do what they can now to pave the way for acquiring certification later.

One widespread trend is for people to acquire entry-level certifications and then move along as their career advances. The retail loss prevention certifications are set up to follow such a logical course.

Gaining an initial designation and then progressing from there makes sense in terms of individual career development as well as the traditional limitations of criminal justice and security as career fields. There is a distinct lack of a visible career ladder within the security industry. This is also true within criminal justice where there is usually minimal relationship between degrees and job requirements. What has occurred within the protective and investigative fields is that certifications combine with progressively more responsible jobs to create a career ladder. Security officers become Certified Protection Officers. They gain more experience, complete the Security Supervision and Management Program and step into a supervisory role. Once there they complete the process for becoming Certified in Security Supervision and Management. After several more years experience they begin studying for the Certified Protection Professional designation. They then successfully take the CPP exam.

In preparing for that exam the previous IFPO programs aided them. So too did the online support from the Foundation. Individual mentoring from a CPOI may also have been a "part of the package." Review courses sponsored by colleges on a credit or noncredit basis may have also played a role.

Professional Certifications: Milestones of Professionalism

Quiz

1. Today, everyone working in the security industry is expected to be a _____.
2. Certification is important because it tends to _____ the individual, much like higher education.
3. Professional certifications may be of use to the individual, the employer, the client, or society at large _____ schools and _____ may integrate them into their curriculums.
4. The IFPO was established in 1988 and makes available the _____ and the _____ certifications for protection officers and supervisors.
5. Membership in professional security organizations allows us to _____ with other individuals.
6. There are few opportunities available today for professional development in the security field. ☐ T ☐ F
7. True professions require advanced education, training, an _____, _____ or experience within the profession. ☐ T ☐ F
8. Professional certifications are the same as user or training certifications. ☐ T ☐ F
9. Membership in a professional security organization helps keep one current in their field. ☐ T ☐ F
10. The final component that an occupational group must have in order for it to be a true profession is _____ by the public.

UNIT V

Management and Leadership

This page intentionally left blank

1 Evolution of Management

Christopher L. Vail

A person selected for a management position usually brings with him/her certain attributes—education, job experience, personal contacts, or a combination thereof. What they frequently do not have is training or experience as a manager. This chapter is meant to provide the basic concepts and framework for new managers, giving them a brief theoretical overview of management, what the manager's job requires, and how to "do it."

The history and evolution of management has given us the framework for what managers do today. Management is nothing new as it has its roots in the beginning of time. Every organization in the world has used, presently uses, and will continue to use some style of management. In any case, regardless of the style used, management has but one question to address: "what is the best way to accomplish our organization's goals and purposes?"

The first studies of management took the classical approach wherein researchers looked at the bureaucratic structures and formal aspects of the organization. For instance, the study of scientific management tried to find the best method of performing a specific task. Frederick Taylor, the father of scientific management, used time-and-motion studies to support his theory that the manager should do the thinking while the employee did the physical tasks. Max Weber's school of thought introduced the concept of bureaucracy. He proposed rational bureaucratic structures that would include written rules, making jobs routine, division of labor, hierarchy of authority, reliance on technical expertise, and a separation of ownership from administration.

A later school of thought in management studies took the human relations approach that emphasized the informal aspects of the organization. The Hawthorne experiments of the late 1920s and early 1930s theorized that if the physical environment was improved, productivity would increase. While this theory was not supported by the studies, it did open the door for studies into variables other than physical ones such as lighting. This, and subsequent studies, suggested that when management pays attention to the employees, productivity will increase. This school emphasizes communication, shared decision making, the recognition of strong social norms in the workplace, and leadership.

There have been other approaches to the study of management, such as the behavioral school, the functional, quantitative, and others. Modern-day terminology includes total quality management (TQM), zero-based budgeting, Theory Z, and management-by-objectives. Despite the fancy name or label, the purpose of management still remains: "how can we best do the job?" In all likelihood, today's manager will use a little of all the schools of thought. Most workplace situations today are complex and are influenced by more than one factor such as globalization, social relationships, physical surroundings, job specificity, or expectations of workers. Therefore, managers should look at the whole picture and match their management approach to the situation. This approach also has a name: situational or contingency management.

Definition of Management

The dictionary defines management as "the act, manner, or practice of managing, supervising, or controlling." Inherent in that definition is the implication that management is not a single, identifiable object; nor is it stable. Management is a *process* of directing and controlling people

and things so that an organization's objectives can be accomplished. Therefore, today's manager needs to be flexible, yet work within the parameters of established managerial concepts.

The Process of Management

The managerial process consists of five functions, each a separate one, but closely tied to the others that tend to operate in a fairly consistent sequence. In short, these functions are as following:

1. *Planning:* setting goals and objectives and developing plans, policies, standard operating procedures, and rules and regulations that will achieve them.
2. *Organizing:* obtaining, arranging, and allocating the right tools, equipment, materials, and personnel to get the job done effectively and efficiently.
3. *Staffing:* recruiting, selecting, hiring, training, and developing an adequate number of competent people, then putting them in the right positions in the organization.
4. *Directing:* activating the employees to achieve organizational goals and objectives through the use of coordination, delegation, motivation, communication, and leadership.
5. *Controlling:* ensuring progress meets organizational goals according to plans by using appropriate reporting systems, performance standards, measuring results, determining and correcting any weaknesses or flaws in the process, and taking necessary actions to gain compliance to bring results in line with plans and rewarding people when deserved.

Planning

The first function performed by a manager is planning. This requires forecasting needs and problems and preparing plans to meet them. Good planning provides the framework for the organization by specifying the "who, what, where, when, and how" to get the job done. Planning, by its conceptual nature, consists of setting goals, objectives, plans, policies, procedures, and rules and regulations needed to achieve the purpose of the organization. Planning requires a lot of thinking before acting. It also means that contingency plans should be in place in the event of emergencies or crises.

Plans may be administrative, tactical, strategic, fiscal, operational, or procedural. They may be long term or short term. Regardless of what the plans pertain to, they will always require detailed thinking and determining what should be done in the future in the organization. One way to assure that all bases have been covered in developing plans is to ask yourself many "what if?" questions throughout the planning stage. Self-imposed questions such as "if we do this, what will happen?", "if they do this, what could happen?", and "if this happens, what should we do?" will suggest an action, or appropriate alternatives, to be taken.

Planning should not be a one-person operation. Using many personnel under his/her command to assist in developing plans has a number of benefits. Involving others in the planning process assures that administrators, supervisors, support, and operational personnel agree on what is to be done. It provides an opportunity to make sure that there are adequate resources available to meet any need. It gives the manager a real insight into what his/her organization can accomplish as a number of different people in the organization will be contributing with ideas, suggestions, and feedback. It is an opportunity for the subordinates to become involved in the organization—an action that tends to motivate people. And, it gives subordinates a chance to see how complex their organization really is and how important they are, as individuals, to the organization's success.

Organizing

The second function of a manager, after planning, is organizing. Organizing means acquiring, arranging, and distributing work among members of the organization so that the goals of the organization can be accomplished. The basic question addressed in organizing is: "how will the work be divided, who will do it, and what do they need to accomplish the work?"

To do this, a chain of command is established that identifies and defines jobs and who will do them. Normally, work teams, units, departments, sections, or other entities are created to perform the task(s). The chain of command also defines the appropriate responsibilities and authorities of people. In other words, it assigns accountability throughout the organization.

An essential element of the chain of command is the principle that authority is always commensurate with responsibility—they must go hand in hand. Clear-cut lines of authority and responsibility will eliminate the problematic "who's in charge?" question. The "golden rule" of management is that no responsibility should be assigned to a person unless he/she has the authority necessary to fulfill it.

The formal chain of command assumes that communications will flow from top to bottom and from the bottom up. Regardless of the formal lines of authority established in a chain of command, most organizations will have an informal one. This is found in the person who just naturally assumes responsibility and exercises authority without anyone spelling them out, such as the file clerk who carries a lot of weight or the mail clerk who knows everyone in the organization. Communications in this informal system may flow in every direction.

A good manager will be aware of and use all communication systems effectively.

The organizing process, particularly when obtaining and assigning man power and the required materials and supplies, should also consider the two different goals of efficiency and effectiveness. Efficiency refers to using the least costly and time-consuming efforts to accomplish the organization's goals and purposes. It is a way of getting the best job possible done at the least cost in time, money, and man power. It is "doing things right" while effectiveness is achieving the desired result, or "doing the right things." While the goal of the manager should be to achieve both efficiency and effectiveness, it is not always possible and one or the other may be sacrificed.

Staffing

The third function of management is staffing. Staffing entails recruiting, selecting, and training employees. Sometimes this function is performed by another organization such as a human resources or personnel department rather than the manager's organization. In this case, the manager can have input into job descriptions that will provide a screening process for acceptable job candidates. Otherwise, the manager will be responsible for recruiting the numbers and types of employees needed.

After recruiting the numbers and types of employees necessary to accomplish the job, the right people must be selected. Questions that are unbiased and job related only should be asked during the job interview to determine if the candidate is qualified to perform the job for which he/she was recruited. Selection of employees should be based upon finding the persons whose qualifications best match the requirements of the job. Resumes should be thoroughly checked. References should be solicited and contacted. Some security positions may require further testing such as polygraph, psychological performance, or other testing methods prior to selection.

The actual hiring may be done by the manager, or again, by the human resources department. At this time, the new employee should clearly understand the job expectations. Company benefits should be explained to the new employee and vacation and sick policies, compensation, insurance, and other employee benefits should be understood by the new employee.

Training, although too often overlooked, is vital to the success of any organization. New employees may bring with them some, a little, a lot, or no training at all for the job for which they were hired. Management should provide, at the very least, minimum training that will assure that the employee can do the job and do it right. From that point on, it is up to the supervisors to make sure that the employee performs adequately. Employee development should consist of an ongoing training program with emphasis on rewarding employees with training, not using training as a "punishment." An important part of the training process should be a new employee orientation program.

One of the goals of staffing should be to assure that the right person is in the right job. After the selection, hiring, and training of people, it may be discovered that the employee is not suitable for the job in which he/she is placed. Training may solve the problem, termination may be a viable answer (also a job of the manager), or reassignment to another job may solve the problem.

A performance evaluation system will detect work-related problems through timely appraisals of each employee's performance. A good system will also point out the positive traits of an employee as well as the negative ones. For this reason, performance ratings can be used as a means of selecting people for promotion, reassignment, or transfer to a higher position if one is available or becomes available.

Directing

This is perhaps the central core of the manager's role in that it includes coordinating people and things, delegating responsibilities and authorities, motivating others, communicating clearly and concisely, and providing strong leadership. Employees look to management for direction; it is in the area of directing that managers "make it or break it." Coordination is merely assuring that the efforts of people and their resources work together to accomplish the goals and objectives of the organization. It is synonymous with directing an orchestra in that one person gets everyone else's cooperation to effectively and efficiently achieve a goal. Coordination is not a "stand-alone" function of management; it is more the result of the manager doing his/her other functions well. It includes aspects of all other managerial functions. During the planning phase, if other people were involved, coordination will occur. In an organization with a well-defined chain of command, everyone knows who they need to work with. With good delegation, coordination is achieved. If the manager selects and places the right people in the right job, coordination will exist. When the manager acts as a leader and motivator, coordination follows.

Delegating authority and responsibility is imperative as a manager. It is far beyond the realm of possibility that one person can perform all the duties and work needed to accomplish an organization's mission. The manager must entrust duties and related authority to subordinates. Lester Bittell and John Newstrom define delegation as "the assignment, or entrustment, to subordinates of organizational responsibilities or obligations along with appropriate organizational authority, power and rights." (*What Every Supervisor Should Know*, 6th ed.)

Not all jobs can be delegated. For instance, the manager may be the only person who has a certain technical, administrative, or skill knowledge, in which case he/she should not delegate a job. Anything of a confidential nature should not be delegated. However, the manager who believes that "if you want a job done right, do it yourself" is not trusting subordinates. Proper delegating allows the manager to concentrate on broader issues and activities. It also gives subordinates an opportunity to improve their job skills and knowledge; it develops employees so that they can learn to handle more responsibilities and provides motivation as the delegated task(s) shows that the manager has trust and confidence in them. Managers do not relinquish control when delegating; in fact, they are still held accountable and responsible for the completion of the task(s).

Proper delegation requires that the manager tells the employees to whom work is being assigned, what they are to do, what you expect from them, how far they can go, and how and when you will be checking on them. Communicate your expectations very clearly and then let the employees do the job. Let them do the job their way. They may make mistakes, but proper delegation (as a part of leadership) allows for mistakes. The manager must focus on the end result, not the process. Therefore, a key concept in delegation is *entrusting* others.

Controlling

Often seen in negative or dictatorial terms, controlling is no more than ensuring that the job is being done according to plans. Controlling is closely tied in with the first function of management—planning. The manager needs to know that the organization's objectives are being met and if not, that appropriate action is taken. The manager must establish acceptable work standards and develop a system of work performance measurements to assure compliance with the organization's plans. When there are deviations, corrective measures should be taken. It is important to have able and capable supervisors to ensure a good control system since they are in more direct contact with the work being performed and the workers performing it.

The One Skill of an Effective Manager

Any discussion of the skills required of an effective manager would take volumes to write about. There are such words as technically and administratively knowledgeable, experienced, dependable, creative, intelligent, and so on. It can also be said that a good manager is tactful, honest, dedicated, has integrity, is fair, understanding, patient, and so forth. Few could argue with any of these. However, one word, perhaps, encapsulates all the skills an effective manager should possess. That one skill is leadership.

Since managers perform five basic functions—planning, organizing, staffing, directing, and controlling—it is clear that they require the assistance of other people. In other words, the manager gets others to perform the actual work of the organization and assures that goals and objectives are successfully achieved. Warren Bennis maintains that managers focus on systems, their structure, and processes while leaders focus on people (*On Becoming a Leader*, 1989). It is *people* that make systems and processes work, therefore, the manager needs to possess and exhibit leadership aptitude just as much as the supervisor who is "in the trenches."

Management and leadership are not necessarily synonymous. There are managers who cannot lead very well and there are leaders who do not always make good managers. Those who manage without demonstrating leadership skills usually will find a high degree of turmoil, misunderstandings, in-house fighting, sloppy or poor work results, and, ultimately, a noticeable loss of productivity and/or profit. Conversely, those who lead find that they usually have a smooth-running operation which produces high results.

There are innumerable qualities that leaders should possess and exhibit. Some of those have been listed above. Other desirable qualities an effective manager should have include excellent communications skills, tenacity, dependability, unselfishness, perceptiveness, compassion, intelligence, and a positive, winning attitude. Of course, the list could go on and on. Roger Fulton, a noted law enforcement author, suggests the most important quality necessary to be a leader is desire. "The desire to lead the way. The desire to take on difficult problems. The desire to go a step beyond. And, of course, the desire to be a leader of others." (*Common Sense Leadership*)

One can manage without possessing any of these qualities, but the results will show the lack of leadership in the manager or in the management itself. The costs of poor management are high: high personnel turnover, low productivity, low morale, high rates of absenteeism and tardiness, rampant rumor mills, and an organizational malaise that refuses to get ahead. On the other hand, when managers are leaders, the opposite holds true.

Summary

As an element of organizational makeup, management, as a function, has been around a long time. Over the years, management has been researched, studied, analyzed, and scrutinized. As a result, a number of theoretical models have emerged to describe the types of management found, such as the classical school of management, scientific management, human relations, behavioral, contingency, and so on. Regardless of which school of thought one adopts or believes in, the bottom line of management has always been, and is to this day, "what is the most effective and efficient way of accomplishing our organization's stated goals and purposes?" This is the one question that management must answer.

Management is defined as "the act, manner, or process of managing, supervising, or controlling." In organizational terms, this means that to answer that question, management is responsible for pulling together the people and resources in the organization to achieve its objectives. Management is seen as a process of directing human and material resources, that is, people and things, so that an organization's purposes can be successfully met.

The process of management consists of five basic functions: planning, organizing, staffing, directing, and controlling. Planning is the initial function of management and should not be seen as a unilateral responsibility or duty. Others should be involved in the planning process since there are benefits to be derived both by the organization as well as the people involved.

Planning is looking to the future and developing plans, policies, rules, regulations, and procedures to assure that organizational goals and objectives will be attained.

The second major function of a manager is organizing. In order to accomplish the objectives of the organization, work must be arranged and distributed among all the personnel. The manager must ascertain how the work will be divided, who will do it, and what they need to accomplish the job. Establishing a chain of command will define appropriate authorities and responsibilities. The chain of command also establishes accountability throughout the organization. A well-defined chain of command not only identifies who does what job and places accountability where it belongs, it also encompasses the "golden rule" of management which is the principle that no responsibility should be assigned to a person unless he/she has the authority necessary to fulfill it.

Staffing, whether it is done by the organization itself or by another human resources department, is a management function that entails recruiting, selecting, and training employees. During this stage, managers must see that the new employees understand all the company benefits as well as job and management expectations. Training employees, especially new ones, is an important part of management and should include an orientation training program. Making certain that the right person is in the right job is a part of the staffing function. Another important part of this function is that of an effective performance evaluation system. A good system will point out not just negative aspects of an employee, but will indicate the employee's good traits and skills.

The last major function of managers, directing, is the crux of the manager's job. Directing includes coordinating, delegating, motivating, communicating, and providing strong leadership. A manager is seen as an orchestra director in that one person coordinates the activities of others by gaining their cooperation to efficiently and effectively achieve a goal. Leadership is the most important skill that an effective manager should possess, for it includes innumerable positive traits and qualities. Management and leadership are not the same for there can be leaders without management skills and managers with no leadership skills. However, efficient and effective managers possess both skills, resulting in higher productivity, high morale, low personnel turnover, and fewer personnel problems.

Evolution of Management

Quiz

1. The theory of scientific management tried to find the best method for performing a specific task. ☐ T ☐ F
2. Management is a process of directing and controlling people and things so that an organization's objectives can be studied. ☐ T ☐ F
3. Obtaining, arranging, and allocating the right tools, equipment, materials, and personnel to get the job done effectively and efficiently relates to:
   a) Staffing
   b) Organizing
   c) Controlling
   d) Planning
4. The principle that no responsibility should be assigned to a person unless he/she has the authority necessary to fulfill it refers to:
   a) Organizing
   b) Leadership
   c) The "golden rule" of management
   d) Effectiveness
5. Considered as probably the central core of the manager's role is:
   a) Planning
   b) Supervising
   c) Directing
   d) Performance evaluations
6. _____ authority and responsibility is imperative as a manager.
7. Often seen in negative or dictatorial terms, _____ is no more than ensuring that the job is being done according to plans.
8. The one skill that an effective manager should possess is _____.
9. Management and leadership are always synonymous. ☐ T ☐ F
10. If an organization is efficient, it will always be effective. ☐ T ☐ F

2

Time and Stress Management

Charles T. Thibodeau and Eric L. Garwood

The lack of adequate time management causes stress and can destroy a career. Stress left unmanaged can cause illness or death. In addition, it can really mess up your day! Because of the seriousness of this topic, this chapter is designed to assist us all with slowing down a little, chilling out, planning our work, and working our plan.

Time management and stress are topics that are very closely related. Just think of the last time you were late for a meeting and racing down the highway trying to get there by 10:00 a.m. with only 3 min to go and you are still 10 miles from your destination. If you had only left 15 min earlier you could have had a stress-free ride to the meeting. This is a very typical stress caused by time management. How many other stressors do you have in your life that can be related to time management? Is it possible that road rage could be the result of poor time management?

The interesting thing about time management and stress is that these two issues are cyclical. That is, poor time management may be caused by stress which in turn is caused by poor time management! The fact that we do not manage our time very well could be a cause of the stress that interferes with us managing our time properly. A person under pressure to meet a deadline is experiencing stress. When that stress peaks they find that time management is just getting in the way and they abandon any hint of managing their time. On the other hand, if that same person starts the day under tremendous pressure, he/she may abandon the time it will take to plan out his/her day and become focused on meeting a single objective. Setting aside planning in the form of time management for 1 day may seem to accomplish one objective but what about the rest of the time for that day?

Poor time management may be caused by stress which in turn is caused by poor time management!

When is the Best Time for Planning your Work?

Each day should *not* start with planning what to do. That should have already been done at the end of the previous day. Before ending any day, whether you are at your office desk or in your den at home, be sure that you spend some quiet time planning the next day. Go over your notes and upcoming calendar of events and have a solid plan for each day before you go to work.

Planning your time is a never-ending job with updates and changes made many times after you have a solid plan in hand. You must keep a calendar and notepad with you at all

times so that you can update your plans periodically throughout the day. That way you can keep track of important business, projects, and deadlines. This idea of having something to write on and write with at all times is very similar to what we teach our security officers regarding field notes. We should follow our own advice.

It appears that the best time for planning your work is the evening before the next day's work. Find that quiet time and build a master plan. Throughout the workday make adjustments to the master plan as circumstances dictate. However, treat that master plan like your road map to success and try not to let anything or anyone sabotage your plan.

This idea of having something to write on and write with at all times is very similar to what we teach our security officers regarding field notes. We should follow our own advice.

Protecting the Master Plan

Time management fails most often when the individual supervisor fails to plan, but there are also those forces in our work environment that attempt to sabotage the supervisor's master plan. At some point, those external forces that seem to be sabotaging the supervisor's efforts to stay on track must be defeated and the master plan followed. This can only occur if there is a plan to start with. The word "management" in time management means controlling the requests for your time. Time management control will include doing the following:

1. Handle the politically charged torpedoes
2. Accommodate any time thievery that will help with your personal or professional advancement
3. Sidestep requests you must handle through delegation to subordinates or by scheduling the request for a later time, and
4. Flat out refuse to take your precious time to be involved with other requests

You know that time management saboteurs will be out there, so a part of time management planning includes planning defensive tactics. While I was writing this chapter, others were preparing for Super Bowl 41. Tomorrow the Bears will be playing the Colts. I can imagine that at some point in the game the ball will be snapped back to the quarterback, and he will want to take his time with the ball until one of his receivers is open to catch a pass. He wants to control his time with the ball each time he takes a snap. However, there are at least six mountain-sized saboteurs from the other team trying to limit his time with the ball. With the proper time management attitude and defensive tactics, that quarterback will find a way to protect his time with the ball until he finds a receiver open so that he can complete a pass. This will all be done regardless of those six time management saboteurs who are trying to torpedo his attempt to manage his time with the ball.

This football analogy is exactly the attitude you must take as a supervisor. As a supervisor you are the quarterback with the ball. The ball is that master plan for time management for the day you are required to maintain if you want to keep receiving a paycheck. The longer you keep that ball to yourself the more touchdowns you will make at work. That necessarily means you will have to fight off those saboteurs who attack your master plan everyday.

We recognized above that you need to be flexible in the administration of your master plan, but never take your eye off the ball. You will want to become real possessive of your time management plan. Do not let anything or anyone take that away from you. The ball is always in your hands when it comes to spending supervisory time. Spend it wisely. Good time management means reduced stress on the job for you and everyone you deal with.

Other Things that Attack Time Management

Although a necessity from time to time, the biggest drain on time management is the time spent in meetings. Meetings mean that people stop producing and meet at a place where they all sit around and talk. There are some supervisors and managers who spend all their time going from one meeting to another. "When it is all said and done, there is much more said than done."

Call a meeting only when it is absolutely necessary, keep the meeting time down to a minimum, always have a meeting agenda, never serve refreshments, move the speakers along quickly, and dismiss the participants as soon as possible so that they can get back to the important jobs they were hired to perform. Do not allow the meeting to turn into a social gathering or a party. Keep it business oriented. It is a good idea to avoid calling meetings if other means of communication are available and avoid attending meetings whenever possible.

All meetings are a drain on time management, regardless of how necessary.

Remember the two important meetings that you will *not* want to miss: attend all politically charged meetings and meetings that will help your future advancement in the company. Other important meetings you should attend include job-related instruction and business planning meetings, professional license and certification credits training, and professional association meetings. Other important meetings should be decided by the totality of the circumstances.

As a point of explanation, politically charged meetings are meetings where your position in the company may be threatened if you were not there. It may be seen as insubordination if you fail to show up at a meeting your boss told you to be at. If you could get fired for missing meetings then for sure attend the meeting. On the other hand, if a meeting will result in exposure to individuals in the company who can make a positive difference to your future, you should attend those as well.

Deadlines can be time management killers. Be sure that when you promise to deliver something that you promise long and deliver short. That is, if you think you can get a project done by Wednesday, always promise it for a Friday of that same week. When you come in early with a project that is definitely a touchdown. Of course just barely meeting the deadline on time might be OK, but finishing the project early is so much better! In addition, when you give yourself a cushion of time like that you eliminate the stress of meeting a deadline at the last minute.

Be sure that when you promise to deliver something that you promise long and deliver short.

Overextending your abilities can also be a time killer. The longer you struggle to complete an impossible task the more time you waste. Never be afraid to admit that you do not have the skills and competencies to accomplish something you are asked to do. None of us want to do this, but reality says that you cannot sacrifice the entire time management plan because your ego will not allow you to admit that you are not up to a specific task.

Good time management then requires you to know your skills and competencies and having the ability to be honest with yourself and others regarding those things you cannot do. This prevents you from getting all bent out of shape with performance stress.

Be honest with yourself and others. Admit it when you do not have what it takes to accomplish a task.

Failure to prioritize is another time management problem. When planning your day you need to be able to prioritize what it is you will be doing. See Table 2.1 for a simple time management form. You may want to set up a scale of first priority, second priority, and third priority or A, B, and C with regards to what you will be doing the next day on the job. Those listed under the first priority column or "A" column will include absolute imperatives that must be accomplished before going home, emergency response, meeting deadlines on deadline day, and satisfying politically charged issues. In the second priority column or "B" column you will have items that are day-to-day care needs like checking on subordinates, writing a measured portion of a long-term project, researching products you have been requested to purchase, maintaining databases, interviewing prospective employees, and other prescribed duties you are supposed to do if you have time. In the third priority column or "C" column you will put the least important tasks including things that if they do not get done that day, there will be no consequences.

Prioritizing will provide a clear view of which tasks to refuse to deviate from when someone asks for your time.

It may be nice to have some free time written into the "C" column for reading, researching, and professional development. That is a great stress-breaker strategy. In any event, having prioritized your tasks for the day will help you defend your plan. You may lose part of your "B" column tasks and all of your "C" column tasks to the time management saboteurs, but you are not giving up your highest priority tasks. Prioritizing will provide a clear view of which tasks to refuse to deviate from when someone asks for some of your time. If all you accomplish are the "A" column tasks in a day, then you may not get a touchdown that day,

Table 2.1 Simple Time Management Form

Name: _____ **Date:** _____

Time	First Priority (A)	Second Priority (B)	Third Priority (C)
8:00 a.m.			
9:00 a.m.			
10:00 a.m.			
11:00 a.m.			
12:00 p.m.			
1:00 p.m.			
2:00 p.m.			
3:00 p.m.			

Note: Obviously this is not a very sophisticated form and many other management information systems exist that provide extensive control of time. This form was designed to facilitate the previous paragraph. The intent was to keep it simple for illustration purposes only.

just a field goal. No matter what, you still got points on the board. You still reduced your highest stress issues for that day.

Phone interruptions are a definite threat to good time management. You can manage your phone best if you have the right equipment. Caller ID is a must. Call forwarding and a good messaging system are also essentials. Screen all your calls and pick up on only those calls that you know will be short. The longer calls will wait until you have time to participate in them. Put longer calls into your time management calendar. Have your administrative assistant call back for you on the calls that absolutely do not need your voice on the line. Unless it is an emergency, strictly business, politically charged, or career-enhancing call, stay off the phone. When on the phone find ways to shorten that call. The problem with the phone is that there is no timer on it and the 2-min call quickly becomes a 15-min one. Four of them and you lost an hour of time that day. Make it a habit to hang up that phone as soon as possible when at work.

Unless it is an emergency, strictly business, politically charged, or career-enhancing, stay off the phone.

Failure to delegate is a time waster. You are a supervisor because you are good at getting things done through the efforts of other people. Delegation of work tasks is actually a motivator. According to Abraham Maslow, one of the founders of humanistic psychology, employees need recognition and the feeling of belonging. By giving your subordinates challenging work you are accomplishing a lot. First of all, you are buying time to be used to fight the time saboteurs, you are motivating your subordinates, you are getting more work done than you could all by yourself, and you are reducing stress.

If you find yourself doing more than you are delegating, you are probably not using the tool of delegation properly.

Dealing with Stress that is not Work Related

To survive in this world of ever-growing stress, we all must develop coping mechanisms. To accomplish this we must start with a healthy lifestyle based on good values and attitudes. For some of us that will be a big task because values and attitudes begin to develop very early in life. Our personality which has a lot of influence on our values and attitudes is said to be set by age 6. In some cases then it will take a personality change to acquire appropriate values and attitudes.

Our basic personality as well as our values and attitudes may lead us in all the wrong directions to reduce stress. Thus, if we really want a life-changing experience in these areas, it will be necessary for us to take a realistic personal inventory of all external stressors that negatively impact us and directly confront them.

It may be a good idea to make a list of all our fears regarding external stress components, like fear of physical confrontation, fear of public speaking, fear of criticism, fear of love disconnects, fear of not belonging, fear of not measuring up, fear of not having a life plan, and just plainly feeling disconnected from society. Some terrific ways of getting reconnected are through returning to a religion, joining a health club, volunteering at a hospital, becoming a tutor after school for elementary kids, participating in one of those Internet love connection

clubs, getting adequate hours of sleep, improving your diet, taking off 50 pounds, and a thousand other activities. The idea here is to get active in the very things you fear. For instance, if you are afraid of public speaking then take a Dale Carnagee course in public speaking.

The worse part of stress is when you are doing nothing to fight it. We cannot allow it to control us; we must take control of it. Some of us quit smoking, quit drinking, clean up our language, and do as many other personal improvement activities as we can think of. We must take care of ourselves and raise our self-esteem. We can do all of these things without therapy. Stress is directly related to your physical and mental conditioning. In the end, we are just about as stress free as we want to be.

Conclusions

From the above it is obvious that stress and time management are definitely interconnected. The stress we experience at work and that which we experience outside work have the ability of combining and tripping us up, no matter where we are. For the purposes of this book we are concerned only with how the clash of internal and external stressors affects our work performance. Of all the stressors we experience at work as a supervisor, stress emitting from mismanagement of time must be considered foundational. External stressors can only exasperate that work–stress experience.

Obviously in a short chapter like this, we can only scratch the surface of this topic and the reader is encouraged to continue this study from the thousands of sources available. If nothing else, begin implementing some of the ideas expressed in this chapter. Your future may depend on it.

Time and Stress Management

Quiz

1. The statement _____ is the first thing you must accept when dealing with time management.
2. Procrastination is the _____ of time management.
3. _____ is the key to time management.
4. When subjected to tension, a natural _____ occurs in the body.
5. A healthy life style is based on good _____ and _____.
6. Planning is essential in time management. ☐ T ☐ F
7. It is appropriate to fight for control of all things in your life. ☐ T ☐ F
8. You should set deadlines for goals. ☐ T ☐ F
9. Effectively managing your time will reduce stress. ☐ T ☐ F
10. Having a good attitude does not reduce stress. ☐ T ☐ F

3

Project Management: An Overview

Franklin R. Timmons

Project management is the art of communication, understanding business, developing processes, and moving them forward. Generally, a project has a defined scope, a certain period of time, and a specific budget.

In a world where businesses are ever changing and companies are being merged, purged, and submerged, project management is a key to the fundamental success of the organization. Often, because of our rapidly changing dynamic organizations or clients, the scope of a particular project will change. When this occurs, the project lead or project manager must ensure that the time period and the budgeted dollars that have been assigned are still appropriate. A big mistake to make is to have the scope expand, but the time period and dollars assigned remain unchanged.

Much of what the project manager does, centers around the ability to improve productivity. Some organizations are in such a constant state of flux, that they have entire groups assigned to do nothing but projects. Many security groups are fastly sculpting themselves in this mold. The customers that they serve, whether internal or external, are requesting an increase in services. Many may be temporary or short term and this is truly challenging many organizations to adopt and adapt to a modified management philosophy.

The individual tasked to oversee these activities is called either the project manager or the project lead. This individual can be someone who is in a more permanent role as a project manager, or can be someone who is picked by the organization to assume a temporary role.

Because projects are ever changing, the project manager must be one who can see the future, understand the needs of the business, and motivate and continuously improve productivity of the team that he/she serves.

Because society has become so dependant on computers and systems, the project manager has to be computer literate and system compliant. The speed at which reports can be generated, and communication can be accomplished, is nothing short of the speed of light. Documents and e-mail can be whizzed halfway across the world in seconds and at half the cost, and reduce the bottom line. Maximizing productivity of people, systems and processes, becomes paramount to the survival of the project manager and the business.

The Good Old Days

Thirty years ago, the emphasis of the project manager was getting the most out of the personnel who worked in various positions. This was done, in some cases, by brute force and a dogmatic disciplinary policy. A"Theory X" management style was commonplace.

Even though financial rewards were sometimes plentiful, the major thrust or concern of the employee was job stability or the "job-for-life" syndrome. The employee knew or felt like they would be maintained by the employer, if the employee maintained a suitable job performance record.

In some cases, employees felt as though they needed an added layer of workplace assurances and in those cases, they voted for and were covered by collective bargaining agreements. The agreements were often viewed in a negative light by managers and seen as the way to preserve a working way of life by the employees.

In actuality, managing to a workforce covered by a collective bargaining agreement is sometimes easier because all the rules are spelled out in writing. Much of what was done was done by seniority, and those most affected by decisions or cutbacks were employees of lesser or least seniority.

Many job functions were not automated and because processes were stable or unchanging, the need for project management was little to nonexistent.

When an occasional project arose, be it a construction project or a process change, a project manager would usually be named from within the organization. They would cease working on their normal day-to-day duties and assume their new role totally consumed by the parts and pieces of their project. Generally, the folks that they interacted with were locals such as themselves, and relationships were already established and in place. The need for outside involvement was limited, because the general knowledge base came from within.

These early forms of project managers had firm understandings of the business and developed true values of wisdom and commitment. They were relentless in their pursuit of excellence, but they were limited by the tools which they were given.

Transition to Today's World

In the 1980s and 1990s, American business continued to evolve. Businesses realized that they could streamline operations and reduce costs by instituting a new policy that would come to be known as "outsourcing." Instead of maintaining their own employees for whom they had lucrative benefit and retirement packages, companies began opting to outsource these positions to contract organizations.

In many cases, the contract companies had little or no benefits, and those that did were substantially reduced from that of the company seeking to outsource. Wages were also less than with the proprietary organization.

Sometimes outsourcing meant the facility closing and physically moving production to other locations and countries, or it meant moving certain functions of the workforce into a contractor role. Often, when the latter occurred, many of the employees who worked for the business, migrated across to the contract company or contract function.

These contract companies continued to evolve across the board in many disciplines. Engineering, maintenance, security, and even entire contract operating companies were examples of this massive paradigm change in the American work culture.

With the advent of this contractor growth, so came the growth of the project manager to manage and lead the work activity.

Project Management: A Security Specific Pie

In the "old days," the senior security person on a job was generally given a paramilitary designation such as lieutenant, captain, or major. Then, often, below them were several more layers of command. There was very little flexibility in command structure and generally situations at the site did not change. Life went as a day-to-day activity and tasks were very manual, at best.

In the 1980's, access control and closed circuit television (CCTV) systems made their way into the picture. Owners of facilities and businesses decided that they could now have a machine fulfill the function of the human being, and do it at a substantial cost reduction.

As we turned the corner on the new century, it became apparent that electronic systems were only getting bigger and better. Globalization was causing businesses to improve their local area networks (LAN) and wide area networks (WAN).

Now, security monitoring stations, command centers, control rooms, etc. began monitoring systems from various parts of the United States and beyond. Access and CCTV systems that

were once hardwired to the central computer server, were now being placed in more remote locations and being controlled over the companies' LAN and WAN.

Officers were now able to complete functions remotely, such as open doors and gates, and communicate with employees in the field and beyond. This capability will most likely continue to expand in the future. It adds a new dimension to what a protection officer is.

The People Piece

The number one asset that any project manager has is their people. These are the people who go out on a day-to-day basis and make the entire program work. It is the people who implement the project. Human resource management is a critical component of the overall project.

The organization can be plagued with high turnover rates that erode the stability and rob the organization of experience and wisdom. This, of course, does not even take into consideration the added costs for continuous processing, training, and equipping new personnel.

Today's project manager is faced with motivating people from a very diverse background and education level. At one point in our past, workforces were generally regionalized and the educational background of the employees or prospective employees was well established. This characteristic is now less common. Because our nation is so diverse and mobile, today's project manager will have to understand a multitude of cultures, in some cases languages, and definitely manage to different academic levels.

Often, these considerations will be directly related to the ability to find a suitable workforce based on hiring requirements and stipulations for the job. Some jobs are slightly more than minimum wage, and often require background checks and drug screens. Many times, even though unemployment rates are high in some areas, the employable workforce for that area, for that specific job category, has already been tapped. Recruitment, selection, training, and retention issues are challenging but must be addressed. A competent workforce must be attained so that the project manager can begin to coordinate the project.

The project manager must communicate, motivate, and lead. They must also identify specific tasks for individuals to accomplish and then hold them accountable. This must all be done in a way that will ensure that the organization and the employees are successful and continue to grow.

Communication

Communication is essential for the success of the organization. The various forms of communication are covered through other parts of this chapter. However, with that being said, it is still necessary to highlight and reinforce several key elements.

Active listening skills are essential. Employees must be heard. And, to be heard, they must be allowed to speak. Listening, many times includes repeat back, the concept of repeating back what it is you thought the employee said to ensure a complete understanding.

After listening, feedback to employees or the project team is the other essential element of communications. Feedback completes the process. It lets the team, either individually or as a group, know what course will be plotted and followed.

Depending on the type of project, status meetings are certainly encouraged. These meetings could be daily, they could be weekly or biweekly. Because some team members may be operating in a support role from remote facilities, a teleconference may be used in lieu of project meetings or project meetings may include teleconferences with remotely located staff. This will have to be determined by the project manager and their team.

Motivation

Sometimes motivating can be one of the hardest concepts for the project manager to grasp and then maintain. Often, the project manager is struggling with their own identity and ways to motivate themselves. The project manager sometimes feels overcome with a sense of futility and helplessness. They may see aspects of the project as being beyond their control. They may feel as though they are "bobbing in the surf"; being tossed and turned by forces larger than themselves.

The project manager has to first motivate themselves and then the employees that they coordinate. This is a continuous and challenging process. It involves understanding, monitoring, and adjustment.

The most important aspect is understanding. This is the first step in the process of motivation. It is essential for the project manager to have a clear understanding of the expectations of the job and the mission. The project manager has got to continuously check and adjust those expectations as roles and responsibilities continue to grow or are modified.

Often, motivation means changing the course, adjusting the way you do business. An applicable saying is, "If you always do what you have always done, you will always get what you have always gotten." If you want it to be different, then the bottom line is, nothing will change unless you change the way you do it, or you change the people you are doing it with.

Organizational Leadership

Leadership is often confused with supervision. A leader is not always a supervisor, but a supervisor or project manager must always be a leader. They must have vision. They must identify tasks and priorities to be achieved.

Leadership includes inherent qualities, such as honesty, trustworthiness, dependability, reliability, perseverance, and being able to ask "what next." A leader is never satisfied with the status quo. The project manager is always trying to improve the status of the project and the position of the team.

Communication is a vital component of leadership. Open, honest, and *frequent* communication is essential in building trust.

Many times, in today's environment, a better organization's chart shows the project manager in the center of a star or circle and has all elements moving around the position versus the standard hard structure organizational chart (Figure 3.1).

Traditional organizational charts were effective in the days of centralized highly focused staffs. But, with today's flexible, decentralized global organizations, project teams need a more elastic and applicable model.

Identify Accountabilities

The project manager is the pivotal person to ensure that goals and objectives are aligned and synchronized. They are the coordinator of the project and must be intimately familiar with the goals

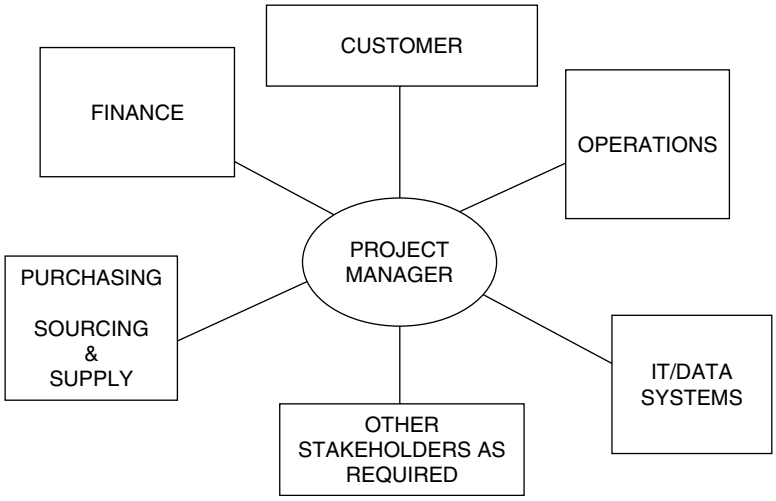


FIGURE 3.1 A nontraditional organizational chart.

and objectives. These goals and objectives must be understood, accepted, and embraced by the project manager. The project manager then must establish priorities and accountabilities that best match those of the company and will lead to successfully attaining those goals and objectives.

Then, the project manager must involve the employees. They must assist the employees in establishing their accountabilities and duties to ensure that the company's goals and objectives are being met. Management's vision must be passed onto the employees. Then the employees' activities must be integrated into the plan.

If these activities are not aligned, there will not be successful completion of required activities. Either the tasks will not be completed or they will not be resolved to management's satisfaction.

Holding Employees Accountable

The project manager is directly responsible for ensuring that the team members get the job done. This can mean that the project manager is maintaining accountabilities for personnel that do not necessarily report directly to them.

At this point, the art of communication, motivation, and leadership are critical.

This can be accomplished through project meetings, reviewing reports, casual interviews and conversations, and actually walking down the project on a periodic basis. This does not mean that the project manager must have hands on experience to ensure compliance and completion. The project manager is often better served by having the team member responsible for that function or area lead the activity. The project manager then acts as an evaluator and can better gauge the status of this particular piece with the status of the total project "pie."

One saying that has particular merit in this situation is "inspect what you expect."

The Program Piece

Managing the program is an essential piece of the pie. For without the program, there is no work. But, you cannot manage a program that you do not understand. So, we have to start by understanding the program.

A project manager must always make certain that they have a clear understanding of the commitments. These commitments are ones that are spelled out in the contract, or various letters or memorandums of understanding. Everyone affected by them should be "in the loop" about them. One method of doing this is to have them on a master list. Once identified on a master list, the commitments can be shared with employees, and the status checked periodically with the client.

Commitments can also be actions or promises made to improve work processes or the general lot of the security force members themselves. They will want to know the status, and here is where that tie back to communications can be made.

Once the commitments are identified, then resources can be allocated to complete the tasks. When we talk about resources, it may mean adding additional staff, or providing training to existing personnel so that they can be cross-trained. Cross-trained personnel can have tasks added to their jobs so that they can accomplish more (job enlargement). Often, we view cross-training as a negative aspect of employment, but if done correctly, cross-training for many employees is seen as improving their worth to the company and ensuring more job security. Cross-training can be motivational, but often, it depends on how it is communicated. Employees must view it as beneficial to them and not as an exploitative ploy by management.

The System Piece

The project manager does not have to be a system's expert, but he/she must have a fundamental understanding of how the systems operate and work to the fulfillment of the mission. The project manager must be something of an engineer, if not a mechanic.

Systems' implementation requires a level of what we call "person/machine" interface. In today's working environment, understanding the system is a crucial function. Additionally, understanding how the system interfaces with the mission and the limitations of the system are also critical.

Many systems are affected directly by the way they are established. It is important to remember that they are only as good as the information that is inputted into them. Another important consideration is the knowledge of what information or reports can be retrieved from these systems. A project manager may expect one thing, but get yet another.

One critical element that today's project manager must address is the contingency plan for the failure of a system or systems. Contemporary protective operations must have viable, tested plans in place for all foreseeable contingency events. Such a capability is becoming an increasingly critical element of protection management.

For example, several years ago, there was a major spring storm that disrupted the activities of a security command center. Two-way cell phones that were routinely relied upon for communication were rendered ineffective when towers were damaged. When phone and two-way radio communications also proved to be less than effective, the young supervisor turned to a project manager and asked "What do we do now?" The project manager identified the fact that once the National Weather Service issued an all clear, runners would be methodically dispatched to open lines of communication. The young supervisor looked in a puzzled way and asked, "What are runners?"

The fact that people physically make notifications versus electronic notifications, was totally unknown to the young supervisor. This young supervisor had never heard of using messengers as a traditional means of contingency communication.

No matter what system is in place, the project manager has to ensure that they know what the contingency plan will be and that all of their personnel know also.

The Business Piece

The project manager has got to be an effective business person. They can never lose sight of the fact that the company they serve, and all the employees, exists to do one thing and that is to make money.

Now, that said, it is an extremely fine line that the project manager walks when he/she is juggling the dollars and motivating the people. As we stated earlier, the number one asset for the project manager is their people. They are the ones who make it work on a day-to-day basis.

Project Management

Quiz Questions

1. Generally a project consists of what three elements?
2. Project is usually very static, with little or no change throughout its life?
3. Today, is our employment situation such that a person can assume that they have a job for life?
4. A collective bargaining agreement ensures that all requirements are covered in _____.
5. Outsourcing has grown substantially in the last 30 years.
6. Card key access system are more dynamic today because they are all hardwired back to the security server?
7. _____ are the most important asset to a project manager.
8. After actively listening, what is the next most important part of communication?
9. "Inspect what you _____."
10. Leadership is often confused with _____.

4

Company Policy and Procedures:

The Security Supervisor's Primer

John T. Brobst, Jr.

Policies and procedures—how many times do we hear these words in our day-to-day activities? Someone is quoting them, breaking them, or needing a new one for some problem or concern that has arisen.

Unfortunately, many security departments run on an antiquated system of "that's how we've always done it" or "there's a memo here somewhere about that." The frontline security officer's duties have grown rapidly in today's society. They are no longer the "guy at the gate"; often times, they are the one responding to crimes in progress, lost children, chemical spills, and fires. A company or security department that does not have a written policy and procedure manual is doing itself and the people it protects a great disservice.

As security supervisors, polices become more than something we enforce. They become an added facet of our job; tools we can use to help us, our employees, and the security department function more efficiently. The focus of this chapter is to help the security manager understand exactly what policies, procedures, and rules are; how they can be written; and, finally, how they are applied and implemented during everyday activity.

What are Policies, and How do Procedures and Rules Influence them?

Webster's Dictionary defines policy "A principle or course of action chosen to guide decision-making."

Policymaking for a security department involves a degree of thoughts and the ability to place those thoughts in a logical and easy to understand document. Policy sets a general outline for a task or idea for a problem or circumstance that an employee will happen upon. For instance, a policy may state; "It is the policy of the Acme Company Security Department to conduct routine patrols of all company grounds and buildings to prevent criminal activity, to locate and report events such as fires, power outages and safety hazards." This statement does not tell the security officer how to patrol, how frequently patrols are to be made, or even to whom to report power outages. It shows that the security department will patrol the area and some reasons why they would patrol. Post orders and procedures take over where a policy stops. The procedure or post orders will tell the officer that patrols are to be made a minimum of three times a shift and to whom to report safety hazards.

Policies can also spell out the stance a company or department takes regarding public and employee issues. For example, a policy may spell out what the minimum requirements are to be employed as a security officer in your facility, or that the company is an equal opportunity employer.

Administrative policies are policies that address a situation that all employees of a facility should be aware of. For instance, a Smoke-Free Workplace policy and an Employee Accident policy are policies that address actions of all company employees. The security supervisor usually does not write administrative policies, but may be asked to provide input into their creation.

Departmental policies address situations or procedures that occur or are specific to a certain department. A departmental policy may be a job description, a call-in procedure, or a use of force policy. This type of policy is the one most commonly written by the security manager.

Procedures are often contained in policies and describe the steps taken to produce a desired result. Not all policies require procedures—for instance, a security policy might state that the department is an equal opportunity employer, or list what the chain of command should be. Depending on what issue the policy is written for, you may have to list a quite lengthy procedure. This is fine if it is thorough and complete. Procedures are more resolute in their function. They are meant to give systematic directions on the actions that are to be performed. The procedure is the most recognizable of all the parts of a policy. In fact, very few policies are written without some form of procedure being contained within it. A procedure often addresses day-to-day activities; for example, signing out a company vehicle, filing incident reports and, steps to follow when calling in sick.

Rules serve a function only when they are made about very simple and clear activities. "No smoking in the jet refueling area" is a very clear, understandable, and sane rule. "Patrol vehicle will be refueled at the end of the shift" and "all incident reports will be completed before going off duty" are more examples. Rules define exactly what employees have to do—no more, no less.

The use of rules in policies can be a double-edged sword. Use them only when absolutely necessary. Overuse of rules tends to discourage the use of discretion and common sense by the officers and often results in them "only doing what I have to do" to get the job done. Not using rules results in mistakes and miscommunication.

In summary, policies give guidelines and are relatively flexible; procedures spell out steps to take to get to the goal, but are more strict; rules are absolutely clear about what can and cannot be done, and are most inflexible. Procedures and rules are generally components of policies; however, rules should only be used when necessary.

The proper utilization of procedures and rules in policymaking provides the manager with an excellent communication tool. Providing employees with current, up-to-date information about what should be done, and how to do it, encourages professionalism and pride in the department and the job function.

Keeping this in mind, let us look at how to begin writing a policy and procedure manual.

Planning

Your task as a manager or supervisor is to create policies, procedures, and rules to address various subjects and situations that your personnel may encounter while doing their day-to-day activities. In addition, you may need to incorporate administrative policies, security policies, and mission statements into your manual. If you have an existing policy manual, review all the policies, taking careful notes about what needs to be changed, deleted, or added. Address these changes with your director or administrator for their input.

When preparing to write a new policy, a few things should be addressed. First, is a policy necessary for the task at hand? For example, writing a policy requiring officers to lock the security office door when it is unoccupied is needless since it is an issue that can be addressed by general orientation.

List the goals you want the policy to achieve. A policy cannot be effective if it only reaches half of its expected purpose. How will your staff follow the policy? Will your policy

be an administrative policy affecting the entire facility? An administrative policy regarding package inspections would affect the entire population of your facility. What goals do you expect it to achieve? Theft reduction for fear of being caught would be one goal. Catching thieves in the act could be another. Be realistic and remember that policies are only guidelines to assist your staff in solving problems.

Will the security policy impact other departments directly or indirectly? A policy changing the times an entrance is locked or opened can affect employees and the public. This change could impact deliveries to your entire facility or just one person. Do your homework and speak with the persons affected to gain their input. Involving other staff gives the added benefit that your new policy will be followed since they feel as if they had something to do with its creation.

Creating a new policy manual will require involving administration, supervisory staff from other departments, and possibly your legal counsel. Writing new policies really only involves one extra step—finding out what you are going to write about. New security policies should address general security matters as well as site-specific problems. Past events will dictate what your policies and procedures should apply to.

Finding a need for a policy is not difficult; every time a new job function or a new post is added, a policy should be implemented if the activity does not fall under an existing policy. The policy may have a general statement to show the stance the department takes on a particular subject, may list a procedure to follow, or have a rule that must be followed to complete the task at hand. Policies should not be created haphazardly and at the pleasure of the manager. Policies need to be applied to situations that are not solved by using common sense or to address specific occurrences at your facility.

Writing Policies

Writing policies and procedures is the easiest part of the entire process. If you have a policy manual in place at your facility, follow the established policy format. Figure 1 shows a commonly used policy and procedure format. The heading block shows the name of the company, to what department the policy applies, the subject of the policy addresses, number of the policy, its effective date, its revision date, and finally the number of pages that should be present. Having the effective and revised dates on the first page will assist the manager when reviewing policies to make sure that they are up to date.

The policy statement is one or two sentences that summarize the goal of the policy. The policy statement should be clear and to the point—any remaining details should be covered by the rest of the policy or a procedure.

The purpose is part of the policy that can be used to further describe the policy statement. In Figure 1, the policy statement shows that security will restrict access to company vehicles. The purpose further refines this statement by saying that the reason is to protect the vehicles and to make sure they are used safely.

Not all policies require the purpose statement. The use of a purpose statement is mostly a matter of company or administrative preference. Some policies, as shown in Figure 2, do not require a purpose statement because the policy statement makes it clear as to what the goal consists of.

A procedure may or may not be required by your policy. Using procedures may add clarity to some policies, while other times they may complicate it. Make the procedure clear and concise—you do not need to write a blow-by-blow description of how to do the task. If you feel a procedure will help to clarify the policy, use one. A procedure can be used when a task is out of the ordinary, or something that the officer will encounter infrequently during their tour of duty. For instance, a burglar alarm at a high-security building may require a different response than an alarm at another building in the patrol area. The procedure for this example could spell out what should be done, who to call, and how the response itself should be handled. Figure 1 shows a procedure for signing out vehicles. It includes rules in its procedure such as where to secure the keys and where to obtain fuel. It addresses various aspects of requisitioning a vehicle, but it does not burden the reader with overly specific or lengthy procedures.

All policies should contain a signature of the person responsible for its origination or directly in charge of the area that the policy addresses. For a security policy, the director or

Policy Number: 1000
SECURITY POLICY
ACME COMPANY Effective Date: 01/01/XX
SECURITY VEHICLES Revised: 10/06/XX
Page 1 of 1

POLICY STATEMENT

It shall be the policy of the Acme Company's Security Department to restrict the use of the Security Department's vehicles to authorized employees.

PURPOSE

To insure the safe use of company vehicles, the safety of employees and to protect company assets.

PROCEDURE

1. Use of unmarked security vehicles by company employees is permitted, provided:
   a) Vehicle use will be restricted to company employees with a valid driver's license.
   b) Vehicle Requisition must be completed with supervisor's authorization.
   c) Vehicle log in the Security Office will be completed with the destination and the time involved.
   d) Trip Sheet in vehicle will be completed with time out/in and mileage out/in.
2. Marked security vehicles will only be used by company employees if:
   a) An unmarked vehicle is not available or about to become available.
   b) Vehicle is required immediately for an emergency.
   c) Use is cleared by the shift Sergeant.
3. In the event non-security personnel utilize a marked vehicle, the Security Officer on duty will:
   a) Place "OUT OF SERVICE" cover on the roof mounted light bar.
   b) Place magnetic "OUT OF SERVICE" placards over the decals on the door panels.
   c) Remove any security equipment in the vehicle and secure it in the office.
4. All vehicle keys are to be maintained in the security office.
5. Unmarked security vehicles will not be used for personal use without the written authorization of the Company President or the Captain.
6. Marked vehicles shall be used for official security business only.
7. Gasoline will be obtained at the maintenance storage shed.

Captain Joseph Jones Jr.

Acme Company Security Department

NOTE: This policy, as with all policies, is intended as a guideline and is subject to change at the Company's sole and reasonable discretion. Policies are not contracts or employment guarantees for any specific duration.

ORIGINAL IMPLEMENTATION DATE: 01/01/XX
ORIGINATING DEPARTMENT: Security
REVIEW DATE: 09/XX
REVIEWED: Capt. J. Jones Jr.
REVISED: 10/06/XX
CROSS REFERENCE:

FIGURE 4.1 Sample policy with procedure.

manager would sign; an administrative policy would require the signature of the company president, CEO, or vice president.

In today's litigious society, it may be a good idea to include a disclaimer showing that the policy is only a guideline and not in any way an employee contract or guarantee of sorts. Speak with your legal counsel regarding policy disclaimers and if they should be included in your policy manual.

Policy Number: 2001

ACME SECURITY POLICY

Effective Date:

COMPANY SECURITY ORIENTATION 02/01/XX

Revised:

Page 1 of 1

POLICY STATEMENT

It shall be the policy of the Acme Company Security Department to conduct a security orientation program for new employees. This program is given monthly as part of the general orientation program provided by the Human Resources Department. The following is a list of topics covered in the orientation;

1. Personal Safety	6. Alarm Systems
2. Security Assistance	7. Incident Reporting
3. Identification Badges	8. Package Inspections
4. Parking Control	9. Crime Prevention
5. Key Card System	10. Additional Information as Required

Captain Joseph Jones Jr.

Acme Company Security Department

NOTE: This policy, as with all policies, is intended as a guideline and is subject to change at the Company's sole and reasonable discretion. Policies are not contracts or employment guarantees for any specific duration.

ORIGINAL IMPLEMENTATION DATE: 02/01/XX
ORIGINATING DEPARTMENT: Security
REVIEW DATE:
REVIEWED:
REVISED:
CROSS REFERENCE:

FIGURE 4.2 Sample policy: Policy only.

Following the disclaimer, you will find various listings, including but not limited to:

1. Implementation date: when the policy came into effect
2. Originating department: who wrote it, or where the policy originated
3. Review date: date policy was last reviewed
4. Reviewed: who reviewed the policy on the review date
5. Revised: when the policy was last revised
6. Cross reference: any policies or procedures that refer to or are referred from the policy

Your facility's policies may include all, some, or none of the above listings. The various dates that list when things were done and who did them are tools that the manager can use when reviewing policies for content, applicability, and timeliness.

Finally, should there be any new forms or paperwork that need to be filled out in order to comply with the new policy, they should also be included as exhibits with the policy.

The format in which policies are written is not as important as the information they contain. However, a clear and concise style for writing policy is important in that it enables the employee to obtain information in a timely and efficient manner, as well as helping the manager maintain the policy as an effective administrative tool.

Implementing Policies

Once the initial policy is written, it may need to go through an approval process until the final written form is produced, distributed, and implemented. Some facilities have a policy review

board in which all policy and procedure pass through for approval. Others may allow the individual department heads to approve a policy, providing that it affects only that department.

Any time a policy is written or revised, a manager should have his director or administrator review the policy with a critical eye. This will assist in finding any problems or items that should be addressed in the policy. In addition, when the security policy affects another department or the entire facility, administration should be consulted and permitted to review the policy for any issues that may need to be resolved.

The new policy has been written, approved, and printed—now its time to implement it. Making sure that the employees read, understand, and know where to find the policy is a concern all managers face when instituting a new policy or procedure. Some suggestions and ideas are included for your review.

Some supervisors post the policy or give a copy to the individual employees and have them sign a sheet (Figure 3) stating that they have read and understand the policy. This sheet, once all the officers have signed it, is filed for the future in the event that a problem arises in which an officer states that they never received the policy. You may attach a copy of the policy to ensure that the employees read it. Use daily briefings or staff meetings to tell the officers about the new policy. You should still have them sign off on a sheet stating that they received and understand the policy.

Making sure that a policy is read company wide is another matter entirely. Issue a memo with the new policy attached to the various department supervisors and have them share the policy with their employees. Although this is not a foolproof method, you will still reach a majority of the employees. Send a general employee memo after the supervisor's memo, telling employees that a new policy was placed into effect and attach a copy of it to the memo.

If the new policy is an administrative or company wide policy, both memos should state where the new policy should be placed and where the employees can find it.

Reviewing/Revising Policies

Unfortunately, policies and procedures are not eternal; duties are added, changed, and deleted. The security manager is responsible for updating the security policy manual to keep it current. Policy manuals should be reviewed and revised a minimum of once a year. This ensures that employees are not getting conflicting information from a new policy when an old one seems to be still in effect.

The easiest way to ensure that the manual is still effective is to update it throughout the year as topics and changes arise. However, it is sometimes difficult to catch every small change as it appears. Read each policy and take notes as to what needs to be changed or removed. Revise the policy and release it just as you did with a new policy. Keep a copy of the original policy as well as each individual revision to it, should a question arise in the future about past practice. For example, a lawsuit is brought against the company for an assault on an employee that occurred 5 years before. The lawsuit states that security was responsible for being in the

TO: Security Officers

FROM: Captain J. Jones Jr.

DATE: 12/20/XX

SUBJECT: Security Vehicles Policy Number 1000

Please read the policy, initial and date the form below. If you have any questions, please let me know. I have read and understand Security Department Policy Number 1000 –

SECURITY VEHICLES.

	Initials	Date
1.	JIB	12/21/XX
2.	ILW	12/23/XX
3.	HBH	12/23/XX

FIGURE 4.3 Employee information sheet.

parking lots at times when employees are coming into and leaving from work after dark. Current policy states that officers are present at all the parking areas to ensure the safety of employees. However, on reviewing the policy in effect at the time, it is shown that employees were responsible for calling security when they needed an escort to their cars.

When discontinuing a policy, for example, a monthly lighting survey that security performed, but now maintenance completes, the supervisor needs to inform the officers that the task is not to be performed. A memo will serve the purpose of informing the officers and any other employees that need to be notified. The discontinued policy should be signed and dated as to when the policy was discontinued and filed for future reference.

The Security Policy and Procedure Manual

The security policy and procedure manual should be as important to the employee for information as their uniform is for identifying them. The manual should be a place to look for guidance in problem situations and as a tool to help other employees with any security concerns they may have. It is your job as a manager or supervisor to make sure that this information is up to date, complete, and available.

As a manager, you should also be making sure that the officers and other employees in your department read and understand the manual. In addition to having the officers' initial and date any new policies that come into the department, they should also be required to read the entire policy manual and initial that they have read it and understand it. This can be accomplished simply by having a sheet posted in the front of the manual with each of the officer's names on it. As they read the manual, they initial and date the sheet when completed; this should be done a minimum of once a year. This also should be done for any other policy manuals in your department (administrative, fire and safety, etc.) to ensure that your staff is up to date on the information contained in them.

Finally, review various policies (old and new) with your staff during training sessions, staff meetings, or daily briefings. Give a little seminar followed by a quiz. Document any sessions in which you covered policy and who attended them. During employee evaluations include a section on knowledge of policy and procedure. All these ideas are tools the manager can use to make sure that employees are aware of the policy manual and how to use it.

In conclusion, policies and procedures guide us, give us information, and are valuable tools that the employee and manager can use to benefit both the department and themselves. Writing policy is not something we look forward to, but it can be one of the simplest tasks to perform. Planning, writing, implementing, and revising are steps we take to make that procedure even easier. A well kept, up to date, and professional looking security policy manual will benefit more than just the department and its employees. It will benefit the company it protects as well.

Quiz

1. Policy is defined as "a principle or course of action chosen to make rules." ☐ T ☐ F

2. Rules serve a function only when they are made about simple and clear activities. ☐ T ☐ F

3. A procedure:
   a) May or may not be a part of a policy
   b) Should be clear and concise
   c) Can be used when a task is out of the ordinary
   d) All the above
   e) None of the above

4. A disclaimer can be used on a policy to help avoid litigation. ☐ T ☐ F

5. Old policies should be shredded when no longer used to avoid confusion. ☐ T ☐ F

6. The manager can review policy with employees:
   a) At the Officer's home
   b) While on patrol
   c) At daily briefings
   d) On lunch break
   e) None of the above
7. The security manager commonly writes administrative policy. ☐ T ☐ F
8. Figure 1, procedure number 4 is an example of what part of a policy?
   a) A policy
   b) A procedure
   c) A rule
   d) None of the above
   e) All of the above
9. Policy manuals should be reviewed and revised at least once per year. ☐ T ☐ F
10. The purpose can be used to further refine the policy statement. ☐ T ☐ F

5 Total Quality Management

Tom M. Conley

Business is changing rapidly. We are now in a global economy and challenges have never been greater than they are now. Progressive organizations are in the process of transforming from the old way of doing business to the new way of doing business. To be successful now, and in the future, it is essential that security personnel at all levels understand the concepts, benefits, and results of Total Quality Management (TQM).

Before we discuss TQM, we must attempt to define it. There is no question that TQM is a hot topic in business and academic circles. Business managers are fervently trying to figure out how to do it while academicians are trying to determine what it is. None of them completely agrees on either the definition of TQM or how to put the concept into practice. This disagreement should be expected. First, TQM is ever evolving as new concepts and methods are developed. Second, different organizations are in different stages of transforming to TQM. Third, different organizations may require different forms of TQM to fit their specific needs.

One notable exception to this pervasive disagreement over the concept of TQM is the definition offered by the participants in the Total Quality Forum, a consortium of business and academic leaders who come together annually to study TQM and disseminate their learnings. A study group of the 1992 Total Quality Forum defined Total Quality as: "A people-focused management system that aims at a continual increase in customer satisfaction at continually lower real cost."

TQM is a total system approach (not a separate area or program), and an integral part of high-level strategy. It works horizontally across functions and departments, involving all employees, top to bottom, bottom to top, and extends backward and forward to include the supply chain and the customer chain.

Not all people will agree with this definition. Some people refuse to acknowledge the existence of TQM, while others are doing all they can to embrace the concepts. Still others are experimenting with TQM and trying to figure out what it means to their business. Whichever position an individual or organization might take, TQM, as a way of doing business. This was used to rebuild Japan in 1950's, not a different way today. This is "old wine in old bottles." is here to stay.

To help us understand where we are now and where we are going, we need to understand the history of TQM. After Second World War, the country of Japan was crippled. Their economy was in ruins and their spirit nearly broken. The United States decided to help them rebuild their economy. A statistician named Dr. W. Edwards Deming, who worked in the US government, was asked to assist on the project of helping Japan. Dr. Deming had previously tried to help companies in the United States, but they turned him away because the US economy was good. There were plenty of workers and since American companies were leading the world's industrial base, they thought that Dr. Deming had nothing that could help them. So, Dr. Deming went to Japan. When he arrived, the Japanese listened. Dr. Deming taught them the quantitative and qualitative concepts of TQM. They learned ways to do things better and at a lower cost while still maintaining high quality. The result of the ongoing work with Dr. Deming was remarkable. The Japanese went from having little or no impact in the global

economy in the middle to late 1940s to having a significant impact by the 1970s. The major difference was the implementation of TQM.

In the decade of the 1970s, the US economy was not doing very well. Inflation and unemployment hit double digits, and American workers continued to want more money and benefits. American companies had lost their competitive edge and were losing in the global economy. By this time, Dr. Deming's work with the Japanese had become widely known and respected by American companies. By the early 1980s, American companies were really hurting. They called on Dr. Deming to help them as he had helped the Japanese. However, unlike the Japanese, most American companies were really not serious about making changes. They wanted a quick fix to their problems. Dr. Deming was selective in terms of what organizations he would work with. And, he would deal only with the top people in an organization. If those top people were not committed, he was not interested in working with them at all.

Finally, companies like Ford, Chrysler, Westinghouse, Harley-Davidson, and Motorola, as well as a multitude of other organizations, came around and were forced to become committed to TQM for their survival. Dr. Deming helped them. The results of organizations implementing TQM and a new way of doing business were both profound and predictable. The profits of companies increased because the quality of their products increased. By the late 1980s, American automobiles were known for their high quality and were priced competitively. People, once again, were proud to buy American.

In addition to Dr. Deming, there have been a multitude of other people during the last fifty plus years, such as Joseph Juran and Peter Senge, who have worked tirelessly to help organizations become competitive and shift to the new way of doing business.

Dr. Deming used a system known as his "14 points for the transformation of management." He used these as a set of guidelines or operating principles for organizational leaders to focus on the changes they needed to make and to keep the focus on continual improvement. Deming's 14 points for the transformation of management are:

1. Create consistancy of purpose toward improvement of product and service, with the aim to become competitive and to stay in business, and to provide jobs.
2. Adopt the new philosophy. We are all in a new economic age. Western management must awaken to the challenges, must learn their responsibilities, and take on leadership for change.
3. Cease dependence on inspection to achieve quality. Eliminate the need for inspection on a mass basis by building quality into the product in the first place.
4. End the practice of awarding business based on the price tag. Instead, minimize total cost. Move toward a single supplier for any one item, in a long-term relationship of loyalty and trust.
5. Improve consistently and forever the system of production and service, to improve quality and productivity, and thus constantly decrease cost.
6. Institute training on the job.
7. Institute leadership. The aim of supervision should be to help people and machines and gadgets to do a better job. Supervision of management is in need of overhaul, as well as supervision of workers.
8. Drive out fear, so that everyone may work effectively for the company.
9. Break down barriers between departments. People in research, design, sales, and production must work as a team, to foresee problems of production and in use that may be encountered with the product or service.
10. Eliminate slogans, exhortations, and targets for the workforce asking for zero defects and new levels of productivity. Such exhortations only create adversarial relationships, as the bulk of the causes of low quality and low productivity belong to the system and thus lie beyond the power of the workforce.
11. Eliminate quotas. Eliminate management by numbers and numerical goals. Substitute leadership.

12. Remove barriers that rob the hourly worker of his right to pride of workmanship. The responsibility of supervisors must be changed from sheer numbers to quality.
13. Institute a vigorous program of education and self-improvement.
14. Put everybody in the company to work to accomplish the transformation. The transformation is everybody's job.

The purpose of Dr. Deming's 14 points is to create a management system that focuses on ceasing some things and commencing other things. It is to create an environment or climate in which employees can work with dignity and take pride in their work.

Dr. Deming's 14 points exemplify a profound new way of thinking for the security manager and supervisor. Under the system of TQM, no longer are we there simply to "make certain" that people are doing their jobs but, rather, the focus is on helping and enabling people do their jobs better through education and support. Ultimately, the objective should be to support the security officer so that officer can support the organization's customer. This applies to proprietary and outsourced security programs.

So what is TQM and how do we use it? It is imperative that the concept of implementing TQM means a fundamental change in the way an organization does business. TQM cannot be implemented simply as a program approach. To be successful and bring the organization and its people profound results, TQM must be implemented as a change in the way an organization does business. In a TQM environment, the key stakeholding shifts from the organization's officers and director to the customer. The organization exists for one primary reason, to serve the customer by providing the absolute best quality product or service for the lowest possible cost. The customer must be the primary concern and focus. If an organization takes care of its customers by meeting their needs, there will be ample profits for all people within the organization.

A key factor to implementing TQM in an organization is that top management must be fully committed to the change. This commitment means that leadership must be provided for TQM efforts inside and outside the organization and TQM efforts must be funded. Without the firm, long-term commitment of top management, TQM will not be effective and the needed changes will not occur in an organization. The result will be that the organization will not gain a competitive edge and, over a long term, they may not be competitive whatsoever against other organizations that do implement TQM as a way of doing business.

Organizations must be effective and efficient in everything they do. Effectiveness and efficiency are vital to understand because they lay the foundation for what we do in an organization. Effectiveness is the impact that an organization's product or service has on the market, whereas efficiency relates to the manner in which we employ resources to produce our product or service. The following two examples exemplify how effectiveness and efficiency work together. Take a company that manufactures carburetors for automobiles. They might make the best carburetor for the lowest price, thus they would have high efficiency. But, where is their market? Cars do not use carburetors any longer—they use fuel injection systems. Thus, their effectiveness would be low because there is no longer a market for carburetors. This is an example of high efficiency but low effectiveness. Take another company who manufactures fuel injection units for automakers. They make a great fuel injection unit but their price is too high, so the automakers purchase their competitor's fuel injection units because they have the same quality, but have lower cost. This is an example of high effectiveness but low efficiency. In order for an organization to compete, their product or service must be highly effective and highly efficient. A combination of both is a competitive advantage and can result in high profits for the organization and the people within an organization. The questions an organization should ask are, "Are we doing the right things?" and "Are we doing things right?" High organizational efficiency and effectiveness is at the core of TQM.

In addition to leadership and a total commitment to organizational change, the concept of TQM involves two disciplines, which are combined and work in conjunction with each other within the concept of TQM. The two disciplines, those who work in a TQM environment must understand, are qualitative methods and quantitative analysis. Understanding qualitative methods and quantitative analysis is important because everything an organization

does involves a process. Some processes are simple while others can be complicated. Typically, the more complicated the process, the more chance or probability there is for errors and inconsistencies to occur. It is the errors and inconsistencies that cause organizations grief and lost profits. Why? Because errors and other inconsistencies affect the quality of a product or service, which in turn affects an organization's growth and can affect their very existence.

Imagine for a moment that you are the president of a company that makes hubcaps for automobiles. You sell your hubcaps to automakers for placement on new cars. It would be important for your hubcaps to be of same size, same color, and it would be important for you to be able to get the hubcaps to the automakers and your customers, on time. As long as these criteria were met and your price was competitive, your organization would probably do well. However, let us say that you had a problem with all the hubcaps being the same color, or let us say the size varied from one batch to another. When those hubcaps arrived at your customer's location, some would not fit on the wheel because they would be too large, while others would simply fall off because they would be too small. Have you started to see how errors and inconsistencies can devastate a business? The key point is that for each process, there is at least one and probably several weak links or a constraint that limits the overall capacity of the process as a whole. Each process is only as strong as its weakest link. Improvement on any other link does not have nearly the impact on the process as does improving the weakest link. Only identifying and improving the weakest link significantly improves the process and thus the organization's performance.

Errors and inconsistencies in a process are known as variance. The employment of qualitative methods and quantitative analysis are used to control variance and keep the errors and inconsistencies in a process within manageable limits. Qualitative methods are an important part of TQM because they deal with the human skills and conceptual thinking part of TQM. While measurement is important, it is leadership and supporting people that ultimately determines an organization's success or failure. This is especially true in the security profession because security professionals are in the people business. While security officers are required to know how to implement the tools they have to work with (alarm, access control, CCTV, etc), it is the people skills that make security people valuable to their employers and customers. Qualitative methods help set the structure for organizational processes. Dr. Deming developed a very effective model known as the Plan, Do, Study, and Action (PDSA) Cycle. The concept of the PDSA Cycle is to plan the work and process, do the work within the process, study the outputs of the process, and then take action on what needs to be changed or take no action, depending on the results. The PDSA Cycle then repeats with the improvement. This model provides managers and supervisors with a scientific method of learning how to make continuous improvements.

The quantitative analysis tools in TQM involve the actual measurement of outputs and calculate variance. Measuring outputs, calculating and tracking variance, and integrating these into a process is critical to an organization's success in a TQM environment. There is no way to control outputs, only input and processes. In quantitative analysis, variance is tracked and measured in a variety of ways. The idea of tracking and measuring variance is to keep the processes "in control." When a process is in control, it means that the variance in a product or service is within the specifications. When the variance of a product or service is out of control, it means that the process has a problem and the output is no longer within the specifications. Take the hubcap example that I discussed earlier. If the hubcap fits properly on the wheel and it matches the color and strength of the specifications, the production process that made the hubcap was in control. However, if the hubcap has a defect in the coloring or strength, or if it will not fit on the tire because it is too small or too large, then the production process that produced the hubcap was not in control or "out of control." The key to consistent quality is to keep the process of a product or service in control. Ascertaining if a process is in control or out of control is determined by statistical variance. Every process has an upper control limit (UCL) of variance and a lower control limit (LCL) of variance. Back to our hubcap example, if the hubcap was too large, it would be above the UCL. However, if it was too small, it would be below the LCL. In both cases, the hubcap would be out of control. The only way for it to be in control, and not defective, would be for the circumference to measure less than the UCL but more than the LCL.

While determining the UCL and LCL of a process is important, it is also important to always be working on the ways that will bring the UCL and LCL closer together, thus always be looking for ways to reduce variance even more than it has been reduced in the current process. It is essential that a process be brought in control before attempting to reduce variance within the process. Traditional methods of controlling variance defined an "acceptable" range of variance. Traditional specifications, used in the manufacturing-based approach for quality, define conformity in terms of upper and lower control specification limits. For example, steel rods should meet the engineering specification for length of 6 in., plus or minus ten one-hundredth of an inch (6 ± .10). This approach tends to allow compliance concerning variation within that range. It assumes that a product just barely meeting specifications, just within the limit, is just as "good" as one right in the middle, but one just outside is "bad." Managers, supervisors, and line personnel must constantly look for ways to improve their systems and reduce variation. In the 1980s, Motorola committed to a campaign called Six Sigma, which is one way of saying that reducing variation so much that the chance of producing a defect is down to 3.4 defects per million, or 99.99966% perfect. The difference between the steel rod manufacturer example and Motorola is that the steel rod manufacturer settled for average variation, whereas Motorola reduced their variance until they had an almost perfect process. By keeping the process in control, constant quality is maintained and defects are minimized. This means that production costs are kept to a minimum and customer satisfaction can be kept high. This is a fundamental objective of TQM. TQM in the security profession is relatively new, but it is coming fast and it is here to stay.

Some of the most common methods and tools used to measure and track processes and variation are Process Control Charts, Histograms, Run Charts, Pareto Charts, Cause and Effect Diagrams, Deployment Charts, Fishbone Diagrams, and Scatter Grams. These tools have their individual purposes and can be used in conjunction with each other. Of course, to be able to employ quantitative analysis tools successfully, the user must have a basic understanding of and competency in general math and basic statistics. An average person normally has the math abilities to add, subtract, multiply, and divide. However, it is less common for the average person to have an understanding of statistics. Understanding statistics is fundamental to being able to implement and understand the tools that are used in the TQM environment.

Security managers and supervisors who understand TQM and know how to work within the TQM system will be well equipped to help their organizations maximize profits and minimize variance. TQM can be used effectively to help security officers in many ways to do their jobs better and contribute real and measurable value to their customers. Long since past are the days when a security officer can come to work, walk around for the shift, and then go home only to return the following day and do it all over again. The employment of TQM in the workplace is a critical process which results in a security officer being able to contribute maximum value every minute of every shift. As security managers and supervisors, it is essential to provide security personnel with that opportunity.

There are several areas in which security managers and supervisors can contribute to their customers. One major area that security managers and supervisors can contribute to their customers is by formulating a value strategy for their customers. Every quality security department or outsourcing organization must have a value strategy to be successful and maximize the money invested in the security program. The value strategy is a comprehensive and well-defined plan that explains exactly how the security personnel from the security department or outsourcing organization will add value to the customer's organization. If a security department or outsourcing organization cannot explain why they should be there and what value they add to an organization, then they are open to budget cuts and being treated with low levels of corporate esteem. A well-detailed value strategy will prevent any "mutual mystification" about what the mission is of the security personnel and will establish a measurement system to track variance and chart progress. With a clearly defined mission, a process can then be developed that will facilitate the implementation of the mission and identify opportunities for continual improvement through variance reduction. It is essential that the value strategy be communicated to everyone in the organization. This will allow security officers to understand the broader mission of why they are on post and what their job really is.

The other major area in which security managers and supervisors can contribute to their customers is to establish and maintain a comprehensive initial and ongoing training program. It is essential that all security personnel, at every level, have adequate security training. Not only does security skills and human relations training provide security personnel with much needed skill sets that enable them to function successfully, but it also provides them with a sense of belonging to a team. Training also provides security officers with a belief that the organization truly cares about them as individuals and what happens to them when they are in the field. Of particular value is the effectiveness of training workers with little or no formal education, many of whom may earn low wages. Such employees have much to gain from general workplace and security-specific training because many lack the necessary skills to compete in an increasingly knowledge-dependant economy that is filled with challenges and stress.

So what is TQM? A closing definition of TQM that personnel in security organizations can use effectively is a management system and philosophy that:

1. Institutes a never-ending process of improvement and innovation.
2. Is aimed at satisfying and exceeding the customer's needs and expectations.
3. Reduces costs through the elimination of waste and eliminating bottlenecks in the organization.
4. Involves all people in the organization.

The focus in all we do needs to be on the customer. The customer needs to be the key stakeholder and understand the value that officers owe, and can add, to their organization for the money they invest in their security program. Anything short of this is unacceptable and will lead to a less than positive outcome. The leadership challenge for today's security supervisor is both daunting and exciting. While the challenges have never been greater than they are now, the opportunity for growth has also never been as good as it is now. The choice of quality is up to each security manager and supervisor. Will you choose quality or mediocrity? One of these two choices will provide the security professional with a satisfying and rewarding career in security that will be a tremendous growth experience, while the other will not. The golden rule is that only the customer is qualified to define quality.

Quiz

1. TQM is an acronym for:
   a) Total Quality Merit
   b) Thorough Quantity Management
   c) Total Quality Management
   d) Total Quality Maintenance

2. Qualitative methods are the part of TQM that deal with numbers and statistical measurement. ☐ T ☐ F

3. Variation is defined as:
   a) a defect
   b) the point halfway between the upper control limit and the lower control limit
   c) an organization's production quotas that are not achieved by the workforce
   d) the errors and inconsistencies in a process

4. The most important aspect of TQM in an organization is:
   a) organizational leadership and supporting people
   b) the measurement of the processes
   c) controlling variance
   d) ensuring that organization quota are met to keep profits up

5. Dr. W. Edwards Deming was a _____ by training.
   a) Math Professor
   b) History Expert
   c) Military Officer
   d) Statistician

6. The upper control limit and lower control limit are essential when determining if a process is, or is not, "in control." ☐ T ☐ F

7. Which of the following is not one of Dr. Deming's 14 points for transformation management?
   a) Focus on increased quotas and reduced defects.
   b) Create constancy of purpose toward improvement.
   c) Drive fear out of the workplace.
   d) Institute training on the job.

8. It is important for people to understand and be able to perform statistics in a TQM environment because:
   a) statistics are the key to understanding qualitative methods
   b) it is really not important for people to understand and be able to perform statistics in a TQM environment
   c) statistical calculations are used to measure and track process variance
   d) it is a key part of being able to be promoted in an organization

9. An organization can be most successful in a TQM environment by measuring and controlling outputs. ☐ T ☐ F

10. The primary reason TQM is effective in the workplace is:
    a) it increases the organization's profits
    b) it reduces operating costs, increases customer satisfaction and increases employee pride
    c) it reduces defects and helps control outputs
    d) it helps customers receive the products they need when they need them

This page intentionally left blank

6 Leadership for Protection Professionals

Christopher A. Hertig, Michael McGough, and Sean R. Smith

Leadership in the Security Industry

As the security industry continues to mature, the need exists for ongoing study of the vital role of leadership within protective operations. An information-based economy that is increasingly international in scope provides new challenges. A dynamically changing threat environment consisting of natural disasters, power outages, pandemics, and computer viruses is confronting both public and private organizations. Terrorism, organized retail crime, commercial counterfeiting, and identity theft threaten corporations and citizens. Security management is becoming an increasingly complex endeavor. Effective leaders are needed more than ever before.

In recognition of this, American Society for Industrial Security (ASIS International) adopted a "Chief Security Officer Guideline" in 2004. Chief Security Officers (CSOs) develop strategies to mitigate risk, direct staff in the identification, development, and implementation of security policies and procedures. CSOs research technological and management approaches to asset protection, and develop relationships with high-level law enforcement, security, and intelligence agencies worldwide. CSOs report to the most senior level in the organization. They must have demonstrated leadership skills, consensus building ability, communications skills, and emotional maturity (http://www.asisonline.org/guidelines/guidelines.htm; accessed on January 5, 2007).

Obviously, candidates for CSO positions will require advanced education, training, and seasoning through years of progressively responsible experience. Professional certification and commitment will serve to round out the candidate. Unfortunately, this may not be happening enough to fill the needs of employers. Downing (2006), writing about the retail loss prevention sector, maintains that over the past several years a number of senior loss prevention positions have been awarded to non-loss prevention executives. His concern is that security professionals are not producing leaders within their own ranks.

This gives cause for concern and action following that concern. Developing future leaders is an immediate necessity. Certainly formal processes such as intern programs are essential in preparing future leaders. Internships can provide undergraduate and graduate college students with a view of how security management processes work. Students can perform both research and investigative assignments, providing the security manager with an additional "set of hands" for selected projects. Internships can also serve as tools for identifying, recruiting, and developing future security leaders. So too are informal, continuous mentoring by persons at the senior levels of the organization. "Passing the torch" is essential for leadership continuity.

Another trend affecting the need for security leaders (at least in North America) is the shifting of public police functions to the private sector. This is occurring steadily due to the breakdown of government bureaucracies that have become largely dysfunctional, the legitimization of private security services, and the perceived need for more crime control measures. There is also the emergence of mass private properties such as malls, colleges, office complexes, and gated communities. The greatest and most persistent driver for this trend,

however, is cost. Public policing is simply becoming unaffordable due to rising salary and benefit costs, equipment, burdensome regulations, etc. A proprietary security department in a mass private property such as a mall or a contracted security company in a housing complex can deliver customized services at a reduced cost. A security service provider can protect a government building, a crime scene, or the site of an emergency better and cheaper than a public police department. Courtrooms are guarded, prisoners are transported, and military bases are protected by private protective forces.

As this trend continues, more and more of our society is being protected by "private security" forces. Against the threat of terrorism or foreign agents, infrastructure protection is needed. Bridges, power plants, and dams must be secured. With 85% of the infrastructure in the United States under private ownership, the burden of securing falls on privately employed protection forces. It can easily be said that: "The greatest issue in public safety is private security."

Obviously, the challenges and responsibilities placed on security professionals are mounting in both scope and complexity. Security personnel need effective leadership and must exercise effective leadership if the challenges of the future are ever going to be met. Leadership is important!

Many of the early policing leaders had military backgrounds from which they derived organizational skills. Security departments are often paramilitary organizations. Many of the early founders of the ASIS International had military backgrounds. Contemporary security industry leaders may or may not have military backgrounds. Many have policing experience. Control forces have historically been public police, private security, and military.

There is also some influence of law in the background of policing and security leaders. Howard Vincent of Scotland Yard, J. Edgar Hoover of the FBI, and several other police chiefs had legal educations. So too have some security leaders such as Timothy Walsh, former ASIS president and noted author.

What is different today is the amount of business management education, particularly at the graduate level. MBAs are becoming increasingly common. Dan Kropp, the 2003 president of ASIS, holds an MBA as well as a graduate certificate in environmental protection and safety management. Kropp did not have a prior military or police background and was the first Society President to not have such a background. He is part of a new breed of security manager with a business management skill set (Longmire-Etheridge, 2003).

Traditional and Contemporary Security Management Competencies

As Table 1 shows, future security leaders will have more business knowledge than at present. They will understand cost issues much more clearly than those of the past. This will blend with and complement the emerging core competency: Security! We are seeing the application of criminological research to crime and disorder problems. As this research matures, it will combine with the more current study of technology. Future security professionals, at all levels, will be better equipped at knowing which crime intervention to apply in a particular situation.

Similarly, the study of natural disasters, accidents, and terrorism loss events is propelling the development of risk methodology. This will coalesce into an emerging science of risk and loss metrics. Due in large measure to these trends, security professionals of the future are likely to have a greater consultative role throughout their organizations.

Defining Leadership

In the latest version of Merriam-Webster's Dictionary, a leader is defined as "a person who has commanding authority or influence." This definition infers formal appointment as a leader. It applies to formal leadership, which is the official title and job description placed on a leader by his or her superiors. Eastman and Eastman (1971) describe leadership as an illusive concept, one that often tends to be confusing rather than enlightening. The rank structure, particularly in a paramilitary organization, provides very clearly denoted lines of authority.

Table 6.1 Traditional and Contemporary Security Management Competencies

Military—organizational skill, necessary for dealing with emergencies. Historically these were civil disturbances. Current and future challenges include terrorism, pandemics, natural disasters	Police—necessary for understanding crime, criminals, and investigation. Also important for forming productive relationships with law enforcement agencies	Administrative—business management is a necessity for understanding the employing organization's assets and risks. Also essential for becoming a member of the management team

One's position in the organization places them in command of others. In reality, leadership exists whenever one influences others to perform in a positive manner. It is both formal and informal.

To get to the heart of the matter—to understand what truly makes a leader—we need to understand informal leadership. This refers to the respect and trust placed in a person by his or her peers and subordinates. Formal leadership makes one a supervisor or manager, nothing more. Formal leadership gives one a title, placing them higher on the organizational chart. Informal leadership is what makes a supervisor's officers willing to follow them and their directives. Bear in mind that the two can be exclusive of one another; many a line officer, lacking any official supervisory duties, has found himself or herself in a leadership position simply because of the respect earned from his or her fellow officers. Additionally, security officers are representatives of management. Others look to them for direction and guidance during normal operations. When emergencies occur their leadership role becomes more distinct. The saying "if you want to lead, you have to take command" is very relevant during emergencies.

Security departments have a variety of leadership roles within them. The bulk of what is written here and elsewhere about leadership concerns personnel at the managerial level. It is important to remember, however, that security officers are, in reality, "adjunct members of the management team": They move up and down the organizational chain of command as dictated by the situation. Officers must have confidence, knowledge, and a positive attitude.

It is also worth noting that today's officers are tomorrow's supervisors. Good leaders understand and embrace this. They realize that leadership is a developmental process. There are few persons who are "born leaders." Security industry leaders are obligated to create an environment where leaders are grown within the ranks.

Table 2 illustrates the many leadership roles in a contemporary security department.

Table 6.2 Leadership Roles Within a Security Department

Director	Articulates vision via Vision Statements, Mission Statements, and policies. Finds the right things for the department to be doing. Obtains funding for department
Manager	Allocates resources. Develops programs, manages liaison with external organizations. Makes sure that things are done right
Supervisor	Leads and inspires subordinates to achieve security mission. Serves as a link between management and line officers, representing one to the other. Line supervisors are the "backbone" of an organization
Security Officer, Loss Prevention Agent, Protection Officer	Directs members of the public. Organizes liaison with internal departments such as Maintenance and HR. Assumes a broader role in emergency situations or when there is no supervisor available. Sometimes referred to as the "after hours Chairman of the Board"

Leadership Activities

There are a number of leadership activities that supervisory and managerial personnel perform. These functions occur in virtually every employment setting; they are universal, generic in nature. Allen (1973) lists them as follows:

Decision-making regarding what to do and in what order to do it. Proper assessment of a situation or problem is essential to supervisors and managers. Personnel in these ranks must be able to "size things up" well. They must be decisive, following through with their decisions, and not vacillating or being hesitant. The order of actions or tasks must be clearly arrayed.
Communicating their decisions and how they want people to carry them out. These must put into simple, easily understandable terms. Proficient leaders are master communicators. They excel at verbal/interpersonal direction. They use frequent informal get-togethers to communicate and strengthen emotional bonds between people (Phillips, 1992). Their writing is precise and articulate. Leaders' writing should also be crafted for the spoken word (Phillips, 1992). Their communication strategies are not limited; they use whatever mediums are available to their greatest effect.
Motivating personnel to carry out their job duties. Leaders who are confident and self-assured do this better. Subordinates must want to follow their directions. The leader who provides a model for others to emulate is most effective.
Selecting personnel or choosing the right people to do the job. This occurs in both the hiring phase as well as in routine operations where supervisors give specific directions to certain subordinates. In security operations, this is a very critical function as the varied nature of job tasks and organizational cultures demands a precise fit between officer and assignment. It may be wise to look for those officers who exhibit leadership potential themselves. It may be wise to select officers that do not agree with their supervisor on all matters.
Developing personnel where the supervisor or manager coaches, teaches, informs, and otherwise educates subordinates so that they become more proficient. Some historical insight into this aspect of leadership may aid us in understanding it better. August Vollmer has been called "the father of police science" due to his promotion of criminalistics in the United States. He also exerted a tremendous influence over police administration and became the leading advocate for police education and training. Vollmer was well known for developing the members of the Berkeley, California Police Department during his tenure as Chief. He believed that police officers did not need an extensive education regarding biology or the social sciences, but that they needed a baseline foundation of knowledge. They needed an understanding. He also saw police roles as multidimensional. Police were to be educated and trained in various areas so that they could become problem solvers.

Vollmer's perspective on the role of the police officer may be relevant to the emerging role of the security officer. Security officers interact with clients. They meet the public. They liaise with supervisors from various departments. They do the same with external organizations such as police, fire, and emergency medical departments. They serve as the agents of the landlord or property manager. They utilize more sophisticated technology than ever before. Clearly a broader education encompassing business management, public relations, marketing, criminal justice, public administration, etc. will serve them well.

Military leaders have often vigorously supported training efforts. United States General John "Black Jack" Pershing was a harsh taskmaster who believed that sweat in training saves blood on the battlefield (Lucas, 1988). His success in the Spanish–American War, Philippine Insurrection, and the First World War may be partially attributed to the emphasis placed on training soldiers. North Vietnamese General Vo Nguyan Giap was a successful military leader, in part, because his men were well-trained. Hans Von Seekt engineered, in large measure, the German "blitzkrieg" by developing the German soldier's capabilities. Under the Versailles Treaty that ended the First World War, Germany was limited to an army of 100,000. Von Seek's army was composed of volunteers who had been carefully vetted. There was a more

comradely relationship between enlisted men and officers than had been the case previously. Perhaps most significant were the 40,000 noncommissioned officers who would become commissioned once the army expanded. When the NCOs were being trained for the higher ranks, so were the officers, platoon leaders were trained to command battalions and majors to lead divisions (Weir, 2005). This enabled Germany to build a large, well-trained army capable of rapid attack—the blitzkrieg or "lightning war"—a strategy which was highly successful.

Obviously those organizations with well-trained protection officers or loss prevention agents will have an edge when comes the time for expansion. A contract security officer who can supervise an account or a loss prevention agent who can assume managerial duties enables the employing organization to expand into new markets. Enhanced capabilities of entry-level security personnel will also aid in responding to an emergency.

Unfortunately in security operations, prejudice, resentment, and egos may come into play. Leading security consultant Charles "Chuck" Sennewald (1985) discusses a syndrome he terms "The Jailer" where the manager holds his or her subordinates back. In many corporate environments, training is not emphasized due to cost considerations. This may also be due to the inflated ego, insecurity, or prejudice of managers against entry-level protective personnel. Such a perspective curtails organizational development. Effective managers must ask themselves if they harbor any negative preconceived ideas about security officers. They should ask themselves if they hold a Theory X perspective toward subordinates, believing them to be lazy, immature, motivated only by money, and needing continuous close supervision.

Effective leaders in the security industry must be devoted to personnel development. They must participate in those activities (training, mentoring, coaching, etc.) that create organizational development over a period of time.

Leadership Attributes

There is a series of characteristics or attributes that leaders share:

Commanding Respect

It has been said that a poor leader demands respect, while a great leader commands respect. A great leader does not have to ask for the respect of his peers and subordinates; he or she earns it by displaying the necessary skills and characteristics, and also by giving respect in return. A leader earns respect by accepting responsibility. Leaders are the first ones into work and the last to leave. A poor leader may ask for respect, but may never receive it due to a lack of willingness to work for that respect. A good leader places his or her own ego below that of the mission, organization, or public to be served. A poor leader does not. Stakeholders such as subordinates, members of the public, internal department heads, external agency heads, etc., see this.

Visionary

Leaders must have visions; at least at the level of Director. They must have a visual image of where the organization is headed and how best to get it there. This characteristic is more important at the executive level, but it is also be present in the mid-level management and supervisory ranks.

During the American Civil War, General Ulysses S. Grant saw that the Western theatre of operations was crucial to Union success. He was one of the first commanders to see this. He also had plans for a concerted campaign on various fronts, a "big-picture" strategic vision of the war effort. The early leaders in ASIS also had vision. They saw much of what the future would demand and set in motion plans and programs for dealing with it. Local chapters for personal interaction and networking, a periodical for the members, and other initiatives were envisioned in the mid-1950s.

At lower levels in the organization, foresight is important. Foresight is a predetermination of where the leader is going and how he/she plans to get there. Seeing the future is essential within any supervisory or managerial role. It is arguably more important in asset protection due to the changing nature of the environment coupled with the dynamic nature of threats against that environment.

Leadership involves influencing others to share the leader's vision and then work toward achieving it. Toward this end, leaders often author vision, mission, and values statements. The vision statement describes what the organization sees itself accomplishing. It provides a description of what the organization will look like in a decade or so. A sample vision statement for a proprietary security organization might be:

> *Will create and maintain a safe, secure, and pleasant work environment for employees, clients, and visitors. The department will partner with employees and clients and attempt to become a world leader.*

A mission statement is a short, concise articulation of what the organization stands for, whom it serves, and how the mission is to be accomplished. It should be developed by participation with employees so that they see it as their product rather than lofty verbiage from those above them. It is not a marketing piece! It is used to direct the activities of the organization. A proprietary security department might have a mission statement such as:

> *Reduce crime and loss by creating effective prevention, detection, and investigative measures in cooperation with both internal and external stakeholders.*

A values statement describes the values and ethical foundation of the organization. It briefly lists or highlights those key attributes that are most important to the organization. A values statement might resemble:

> *Honesty, integrity, perseverance, and respect for the rights of others.*
>
> *Dedication, teamwork, and continuous self-examination in the pursuit of excellence and professionalism.*

Entrepreneurial

Leaders at the upper managerial level are entrepreneurial. They organize, manage, and assume the risks associated with running an organization. They must understand the importance of order and organization (Finneran, 1981).

When the visionary aspect of leadership marries the organizational aspect, great things occur. A foundation in the liberal arts may be important in developing vision. Through an appreciation of history, philosophy, and the study of different cultures, a future leader can gain perspective. Such a liberal arts background also provides breadth and enhances credibility.

Henry and John Fielding, Patrick Colquhoun and Allan Pinkerton were entrepreneurs. Each envisioned a police or security force structure, organized, and managed it. They were pioneers who devoted much of their time and funds to these ventures.

Henry Fielding, a playwright and novelist, became a magistrate at Bow Street in London in 1748. Crime and disorder were rampant. No one dared to walk alone unarmed at night, and homes were armed fortresses. The control forces of the day consisted of parish constables and nightwatchmen who were ineffective. On those occasions where serious trouble arose, troops could be summoned, but only after the fact. Property destruction, arson, and sometimes murder had already occurred (Reith, 1956). Fielding envisioned a new type of crime control system of citizen householders who went into the streets as a sort of neighborhood watch. This group was much more active than contemporary neighborhood watches as they apprehended lawbreakers and brought them before Magistrate Fielding. Fielding experimented with a small body of handpicked men who affected miraculous results in the neighborhood. Eventually they became the Bow Street Runners, an organized detective force.

Patrick Colquhoun was a successful and enterprising merchant whose greatest interest was social reform; in pursuit of this, he sought and obtained appointment as a magistrate (Reith, 1956). He endorsed three ideas originally proposed by the Fieldings. These ideas are readily apparent within contemporary police and security organizations:

1. The police should have an intelligence service for gathering information about offenders.
2. There should be a register of known criminals and unlawful groups.

3. A police gazette should be published to aid in apprehending criminals and publicizing punishments (Peak, 1993).

In 1798 he initiated a grand experiment in policing with the formation of the Thames River Police. The Thames River Police was organized to curb the thefts that plagued the world's largest port. Two features of the marine police were unique. First, patrols were preventive with officers patrolling in a visible manner to deter thefts. Second, the officers were salaried and were prohibited from taking fees. The venture was a complete success, and reported crimes dropped appreciably.

Colquhoun's Thames River Police were the first regular professional police force in London. The force was funded in part by the government and in part by the West India Trading Company. Public funding began in July 1890 when the House of Commons passed a bill making the marine police a publicly financed organization (http://www.britannica.com/eb/article-36618/police; accessed on November 11, 2006). Colquhoun's ideas on public–private partnerships represent a historical example of the type of protective organization that is increasingly common today with public funding of contract security services. His Thames River Police followed a particular model; future protective arrangements will follow similar models.

Colquhoun was inspired by the work of the Fieldings and wished to take it to a new level. He wrote extensively about the need for a preventive police force, publishing "A Treatise on the Police of the Metropolis" in 1795. While Colquhoun succeeded in establishing the Thames River Police within his magisterial district, he was never able to implement his policing scheme on a grander scale (Oliver and Hilgenberg, 2006). At the time, severity of legal punishment was thought to be the sole means of crime control. Colquhoun died in 1820. After his death, the goal of creating a police force was taken up by Robert Peel who became Home Secretary in 1822. Peel had witnessed the failure of legal sanctions and military repression in controlling crime (Reith, 1956). He drew on the earlier work of the Fieldings and Colquhoun and began to propose the creation of a police force. In 1829, the Metropolitan Police Act was passed by parliament and Peel was placed in charge of the agency created by the Act. Peel immediately hired two men to run the department: Charles Rowan and Richard Mayne (Oliver and Hilgenberg, 2006). Both had military training and initiated a force of a thousand officers organized within six divisions (Reith, 1956).

Peel has come to be regarded as the "Father of Policing" (Oliver and Hilgenberg, 2006). The Nine Principles of Police developed by Rowan and Mayne have been attributed to him. These Nine Principles have served as guidance for modern police departments in England and America. The Nine Principles have been paraphrased below:

1. Prevent crime and disorder. Police do this instead of military forces and severe legal punishments.
2. Recognize that the power of the police to fulfill their functions is dependent on public respect and approval.
3. Securing public respect also means securing the willing cooperation of the public in complying with the law.
4. Recognizing that the extent of public cooperation and support is diminished proportionately by the use of force and compulsion to achieve police objectives.
5. Seek and preserve public favor through impartial enforcement of laws, not by pandering to the public. The police are to be independent in their service to the law. Police are to readily offer service to all members of the public. They are to be courteous and readily offer individual sacrifice in the protection of and preservation of life.
6. Being judicious in the use of physical force. Applying force only when necessary to achieve a police objective. Using force only after persuasion or warnings have failed. Using only the minimal amount of force necessary.
7. To maintain a relationship with the public which recognizes that the police are the public and the public are the police. Police are only members of the public being paid to give full-time attention to those duties that are incumbent on every citizen in the interest of community welfare.

8. Recognizing the need for strict adherence to police-executive functions without even the appearance of an attempt to usurp the powers of the judiciary.
9. Recognizing always that the test of police efficiency is the absence of crime and disorder, not visible police actions in dealing with crime and disorder.

These Principles are, or should be, relevant to the administration of security forces, be they contract or proprietary. Persons in leadership positions or those aspiring to advance into such positions should contemplate the Principles as they may be applied to present or future assignments.

Allan Pinkerton, a Scottish immigrant, founded a detective agency in America in the 1850s. It was probably not the first such agency, but it was unique enough and well managed enough to grow into the largest security and investigative entity in the world. Pinkerton's early clients were railroads and governments. His agency offered both investigative and guard services on an international basis. With branch offices in Chicago, New York, and Philadelphia connected by telegraph, he had rapid communication. As the agency added branches elsewhere, his agents could respond to client needs where his competitors could not.

Pinkerton took the technique of using undercover agents—"assuming a role" and used it to great effect. In some cases he had numerous agents assigned, each obtaining pieces of evidence. He also used the first female investigator, Kate Warne, a good 60 years before any female police were employed in England or America. In addition to Ms. Warne, he had other female agents in the Female Detective Bureau (Mackay, 1997).

His sons William and Robert carried on his entrepreneurial endeavors. The agency delved into providing investigative and security services related to labor unrest. North American companies in the latter nineteenth and early twentieth centuries had serious problems with labor union violence. This included various acts of terrorism such as murder, sabotage, and arson. There were mob actions in the form of massive strikes and riots. While much of this business would not have been accepted by Allan Pinkerton who was a staunch supporter of organized labor, it did exploit an expanding market. In so doing, it helped to make the Agency a large and successful business.

In 1970, Lewis (Lew) Shealy convinced officials at Woodward and Lathrop to install the first pan, tilt, zoom camera system in an American department store. He also devised a way to install a camera in the head of a manikin so that the lens took the place of an eye. Both innovations were effective; today these techniques are commonplace. In addition to his work with cameras, Lew Shealy led a handful of merchants in setting up a sting operation in conjunction with the Cook County Sheriff's department. This simulated fencing operation culminated in the arrest of hundreds of Chicago area shoplifters and the recovery of millions of dollars worth of stolen merchandise (Trlica, 2006).

The leaders discussed above, all held down positions of substantial responsibility. They either were executives within an organization or were running their own business. They all demonstrated vision married to organizational skill. As contemporary protection requires creative approaches that may involve substantial funding, organizational redesign, or public awareness, vision and the ability to execute that vision will become even more important.

Influential

Leaders are, above all else, influential. They impart their visions, their views, on how things should be to others. Leaders often write and publish. They teach. They are involved with professional organizations. They mentor. They promote professionalism both inside their industry and to the public at large through a variety of methods. They motivate others to follow their visions. Ultimately, the visions are carried out. There are many historical examples of leaders in policing and security influencing others.

Henry Fielding was involved with several periodicals and wrote the famous novel Tom Jones. Patrick Colquhoun, though not as well known today as Fielding or Peel, was influential, however, authoring various books and pamphlets on the prevention of crime and disorder through the use of preventive policing. Allan Pinkerton authored a total of 18 books; although only 5 may be regarded as solely his own work (Mackay, 1997).

Pinkerton also believed in cooperation between police departments at the national and international levels. His sons Robert and William continued these efforts. In 1894, an asso-

ciation of the chiefs of police from various US and Canadian cities was formed, later known as the International Association of Chiefs of Police (IACP). William A. Pinkerton served as a governor of its board from 1898–1924 (Horan and Swiggett, 1951).

In the late 1990s, Pinkerton's advanced the Certified Protection Professional (CPP) for their managers. After being acquired by Securitas, the tradition continued. Securitas sponsors managers to take the certification exam. They also have some preparatory materials for their managers. In their job descriptions they list the CPP as a desired qualification for Area Vice Presidents.

Today, Don Walker, CPP, the Chairman/CEO of Securitas, continues to be a driving force behind the National Association of Security Companies (NASCO). Securitas has maintained a leading role in NASCO, an organization of the largest US contract security service providers. NASCO seeks to build relationships within the security industry, improve standards, and assist in publicizing the services provided by security personnel and increasing cooperation between law enforcement and private security (http://www.nasco.org/about.php; accessed on July 1, 2006).

Tim Walsh, JD, CPP, served as the 10th President of the ASIS International. He became president of the newly formed ASIS Foundation in 1967. He and his friend Richard Healy coauthored the Protection of Assets Manual, a massive four (4)-volume publication covering numerous aspects of security that is used as a text for the CPP designation. Tim Walsh was also instrumental in establishing the CPP program. He is well known as a writer and consultant within the security industry (http://www.questia.com/PM.qst;jsessionid = FtyNZSN51p rqxzglK1gnnxvH6Q2Yps2s5nKnJLxvsTjTlnBXWQDw!48714160?a = o&d = 5002160538; accessed on January 5, 2007).

Ron Minion, CPP, CPO, founded the International Foundation for Protection Officers (IFPO). He served as a Regional Vice President for the ASIS International. At the ASIS International Annual Seminar & Exhibits the popular "Canada Night" meet and greet function was started by Ron Minion in 1985. He also had several magazines that he published and ran a training academy. He was the first CPP by examination in Canada. He saw the need for professionalism in the security industry at both the entry and managerial levels. Minion then put a substantial amount of his time, effort, and finances into the magazines, academy, and Foundation.

Lew Shealy of Marshall Fields and Eckerd Drugs played a key role in expanding the Stores' Mutual Associations, often sharing his knowledge with other loss prevention professionals at local meetings and national conferences. He also became a retail spokesman, appearing on the television program 20/20 where he pointed out that retailers were serious about the shoplifting problem (Trlica, 2006).

Charles "Chuck" Sennewald, CPP, CSC, served as a Security Industry Representative of the US Department of Commerce, visiting various foreign countries. Chuck also served on the original Board of Directors of the IFPO. He later founded the International Association of Professional Security Consultants. The Association developed a professional designation for security consultants, a step designed to identify true consultants from vendors (Zalud, 2006). He has authored five (5) books on security management, consulting, and retail loss prevention.

King Rogers served as Vice President of Asset Protection for Target Corporation. He has served on numerous councils and has been involved in various security organizations. King aided in developing the Internet-based Master of Science degree in Criminal Justice with an emphasis in Security Administration at Michigan State University (http://www.kingrogers.com/team_rogers.html; accessed on January 5, 2007).

Some contemporary leaders see a need to influence and educate those outside of the protection business. Certainly upper management must understand the purpose and practice of protection. So too must various other publics. This includes end users, be they clients, tenants, or customers who have purchased equipment. These publics must understand threats that face them as well as how to best manage those threats. Unfortunately, news media, entertainment media, and marketing campaigns by security providers may confuse them. Education also includes those who may someday join the protection industry. Speaking to groups of high school and college students about privacy and identity theft, organized retail crime, terrorism,

and other emerging issues are important. It may be argued that the influential role of leaders in security is needed now more than ever before.

Transactional and Transformational Leadership

Transactional leadership is primarily concerned with maintaining the present operations of the organization. Transactional leadership is more closely related to management.

Transformational leadership is change-oriented. It begins with a vision and through a series of carefully designed steps creates a new organization.

Transformational leadership is necessary in those organizations which are new or troubled. It is not uncommon for security managers to accept a director position and have to design and develop a protection operation from the ground up. Starting a new security program or radically revising an existing one is a common situation for a director to be in. Doing one's research on the culture of the organization is important. So too is knowing the organization's history. Organizations, like nations and individuals, are to some extent "captives of their history." They tend to repeat their history to a large extent and not go into radically new directions. Sometimes being brought into an organization with marching orders to "clean house" is not as strong a mandate as the new manager thinks.

There are also budgetary constraints. New managers may be given virtually every resource they request—for a time. Once the "honeymoon period" is over their requests are denied. What appeared to be extremely strong, organization backing now is put into perspective. The length and degree of the free spending period varies with each situation; the astute leader recognizes this.

It is also common for managers to move into organizations that have substantial difficulties. These can be the result of scandals, dysfunctional organizational structure, or the problems associated with rapid expansion into a new market or area. Contract service firms may expand quite rapidly with a stretching of the span of control. This in turn may lead to an inefficient chain of command. It may also become necessary for contractors to eliminate or not replace supervisors as a cost-cutting strategy. The organizational effectiveness of an operation must always be critically assessed by someone stepping into a new leadership role.

One concern is that security managers have accountability for major business decisions. In particular, IT-related issues if not handled properly can threaten the survival of the business. Failing to secure information properly can expose an organization, whether private or public, to extensive civil and criminal liability. These developments create pressure on CSOs to make important decisions. A cardinal rule is that business decisions should be made by CEOs. Security directors should advise with factual data and opinions if asked for them. This keeps them in a consulting role as is appropriate to their job description.

Another transformational management concern is changing the values of an organization. This obviously takes time. Leaders must impart ethical beliefs and behaviors incrementally and continuously. Trautman (1993) recommends the following for mid- and upper-level managers:

- Being supportive of sound ethics but not controlling
- Promptly responding to questions regarding ethics
- Making ethics training available when it is needed
- Utilizing MBWA (Management by Wandering or Walking Around)
- Recognizing and rewarding ethical conduct
- Emphasizing team effort over individual efforts
- Viewing each and every ethical dilemma as an opportunity to do the right thing rather than a crisis or problem to be avoided

Ethics are essential to the long-term success of any organization. Effective managers and supervisors know this and internalize it. They take every opportunity to teach it to their subordinates and colleagues.

Leadership Skills and Traits

There are some key competencies that leaders must have in order to be complete and well-rounded as leaders. These skills and traits are necessary for a leader to command respect. Persons at the supervisory or managerial level must have these attributes in order to be successful:

Technical Skill It is self-evident that, in order to set a good example for his or her subordinates, a leader must have a clear understanding of, and a high level of competence in, his or her job. Leaders are often chosen from among those with the highest levels of technical skill because in many cases, these are the ones most respected by their fellow officers. They are also the ones who the organization would like its officers to emulate.

Technical skill adds greatly to one's self-confidence, as well as the confidence that others have in him or her. Also like confidence, skill is very often increased by experience. However, a member of the asset protection community has many other options when it comes to increasing his or her skill level.

One's own organization is likely to host many in-service training sessions on a wide variety of topics; this is in addition to the long period of classroom, field, and on-the-job training that is common for new hires of most agencies. When an officer chooses to accept a position of leadership, his or her organization may organize another training program to encompass the new duties and responsibilities he or she will be expected to fulfill.

However, it would be foolish for an officer to stop with the in-house training offered by his or her own organization. Indeed, one of the characteristics of a good leader is a willingness to learn, to absorb new skills and new perspectives. Moreover, a good leader knows that the learning process is continuous, lasting one's entire life.

There are a vast number of organizations which offer training programs to safety and security professionals. These include the IFPO, the ASIS International, the Crisis Prevention Institute, Professional Security Training Network (PSTN), AST Corporation, etc. Some of these training programs may be integrated into in-house training sessions, others may be optional, but offered free of charge or at a deep discount through one's employer. Members in professional organizations receive discounts; membership in IFPO entitles one to substantial discounts on Foundation, PSTN, and AST programs. A leader takes advantage of these golden opportunities as often as he or she can!

Continually honing one's technical knowledge, skills, and abilities are an inherent aspect of professionalism. They are of even greater import for those in leadership positions. Remember the adage:

All leaders must be readers.

Interpersonal Skill Memorize this fact: a leader is a "people person." A leader has different responsibilities to superiors, peers, subordinates, and customers. In order to fulfill these responsibilities, he or she needs to interact with these people on a regular basis. Failure to do so effectively will lead to a lack of understanding of their issues and, of course, the issues of a team are the issues of their leader. Empathy—the ability of one person to understand others by seeing himself or herself in their shoes—is an essential trait for a good supervisor to possess.

However, the ability of a leader to understand his or her personnel and customers means nothing unless he or she is able to communicate with them. Communication is absolutely critical, and takes countless forms in the workplace. Here are just a few examples:

- *Explaining orders and assignments*. A leader must ensure that his or her orders are carried out, which means clearly explaining each task so that there is little or no room for error. In addition, it means explaining why those tasks must be carried out; officers who understand the reasons behind their duties are more likely to take pride in those duties, ensuring that they are performed more effectively. In security operations it is essential that officers and investigators mirror the parent or client organizational culture. Leaders in protective operations must be adept at explaining that culture, complete with all its nuances.
- *Discipline*. It falls to a leader, on many occasions, to discipline his or her subordinates who make mistakes. Discipline may range from a verbal reprimand to instant termination, depending on the behavior. The most important thing to remember about discipline is that it is far from being punishment for its own sake; it must cause a positive change in behavior. It must also be accompanied by an explanation of why the discipline is taking place, and how to avoid such situations in the future.

- *Training*. Continuous training is excellent for all employees; it increases their levels of skill, confidence, and motivation. Not every leader is directly involved in the formal training process, but every leader teaches his or her subordinates various things, at least indirectly. Whether by explaining the proper way to perform a certain job function, discussing current issues related to the field, or simply setting a good example, a good leader makes it his or her business to teach his or her subordinates whenever the chance presents itself.
- *Casual conversation*. Finally, one of the best ways to improve the bond between a leader and his or her team—thereby improving morale and trust—occurs very naturally during the course of a shift. A simple, casual conversation between a supervisor and a subordinate works wonders for these purposes, and lightens the mood in an often-stressful workplace. It also affords both parties an opportunity to learn about one another, paving the way for increased empathy when it is needed.

Confidence. No one can be expected to feel confident in a leader who does not feel confident in himself or herself. A good leader exudes confidence at all times, even when faced with extremely stressful situations. One might say that good leaders exude confidence especially in such times because this is when their subordinates and the population they serve need them the most. A confident leader inspires that same confidence in his or her line officers, improving both their morale and overall performance.

Especially in the public safety field, the ability to make extremely quick—but also correct—decisions is critical. A high level of confidence is essential in these cases. A leader who lacks confidence may waste a great deal of time hemming and hawing, risking both the respect of his or her peers and, potentially, the safety of the population.

Confidence, of course, comes in part from experience. There is no substitute for experience; we are all much more confident about handling a situation if we have been through that situation, or a similar one, in the past. It is for this reason that most officers are not promoted to supervisory positions without having been with their organization for a year or more. However, a leader must ensure that he or she is able to handle any challenge—even one never encountered before—and must guide his or her team to do the same. In order to maintain confidence and effectiveness in these situations, preparation for any event is the key. There is a lot of wisdom in the old saying, "He who fails to plan plans to fail."

Finally, let us remember that confidence does not equate with arrogance. No matter how adept a supervisor may be, he or she must never become cocky. Failure to be on guard against arrogance may lead to a number of problems, including:

- Too much complacency in one's abilities, which leads to laziness
- Rejection of assistance and advice from peers and subordinates
- Disrespect for one's coworkers and/or customers
- Unethical activity, guided by the belief that one won't be caught
- Unwillingness to participate in tasks that one considers "beneath" him or her

Any of the aforementioned problems will severely compromise a person's ability to lead. Confidence is one of a leader's greatest assets, but bear in mind that "pride goeth before a fall."

In order to develop one's confidence there are several steps which DuBrin (1988) offers:

1. Obtain a few easy victories. Once some Athletic coaches understand this; in particular, managers of professional boxers have a keen appreciation of the importance of "bringing a fighter along" with a series of victories over progressively more challenging opponents.
2. Enter a less competitive environment (arena). "No one can be a champion in every arena."
3. Attack situations assertively. Always being positive about things, having an upbeat attitude, and doing that which is productive.
4. Achieve something that stretches one's capability. Challenge oneself in new areas.
5. Take an inventory of one's personal assets.

6. Ask others about one's good points. This must be done very carefully!
7. Dress to feel confident. One old adage is to "dress at the level you wish to attain."
8. Raise your self-expectations.
9. Avoid making negative comments about yourself.

Management Skill. Management and leadership are distinct, but related functions. Huffmire and Holmes (2006) maintain that leaders do not necessarily have to be adept at management, but that great leaders are great managers of personnel. The addition of managerial skill propels one to a new level of leadership. Certainly one can be charismatic and inspire others for a short duration; but to head a large number of personnel over time requires administrative expertise.

Ethics. A leader must set the standard for his or her subordinates in terms of ethical conduct. This is imperative! According to Fulton (1995), "subordinates will emulate, consciously or subconsciously, their bosses." Line officers will see a supervisor with uncompromising integrity, and will not only respect that integrity, but will begin to reinforce that same integrity within themselves. However, if officers observe a supervisor who violates rules or bends the truth, they will begin to see those behaviors as acceptable, and will commit the same behaviors. Such influence may be felt several layers down in the organizational structure. A corrupt CEO can severely damage an organization.

One aspect of ethics in leadership is being ethical in times of crisis. Economic challenges may present a major temptation to engage in less than ethical business practices. Wittmeyer (2003) states that management integrity is essential during periods of uncertainty. Managers with integrity are able to attract and retain capable, trustworthy employees. They command respect and gain support in times of crisis. As a result they can build enduring relationships with various stakeholders.

At the other end of the spectrum, leading with integrity during periods of prosperity can be an ethical challenge. Management guru Peter Drucker maintained that it is easy to lead during good economic times; that adversity is the true test of leadership. He further warned against crooks running organizations during economic boom times: after the ensuing scandal these individuals go on trial. Firms with leaders who have integrity survive and prosper during boom times and the recessionary periods that follow (Zahra, 2003).

Abraham "Honest Abe" Lincoln was, with few arguments, one of the greatest leaders in the history of America. A large part of his leadership ability, and the respect we still have for his reputation today, came from his honesty and integrity. He knew how difficult it is for a person to respect someone who is dishonest, and if a person cannot be respected, he or she cannot be an effective leader. He spoke out both publicly and privately against those he considered to be cheats and liars, and fired his own secretary of war because of his less-than-honest practices when awarding defense contracts.

Security industry leader Allan Pinkerton was an associate of Lincoln's from before the War when Lincoln was legal council for the Illinois Central Railroad and Pinkerton provided security services to the Railroad. Pinkerton is remembered for initiating a code of conduct called the General Principles when the Pinkerton Agency was founded in 1850. This code was well ahead of its time as it forbade accepting contingent fees, gratuities, or rewards, a practice which was common among public police departments at the time (MacKay, 1997).

Remember the words of James MacGregor Burns:

> *Divorced from ethics, leadership is reduced to management and politics to mere technique.*

Leadership Styles

There are three basic styles of leadership. Each leader will have his or her own preference based on their individual personality. Other determinants will be the relationship with subordinates, size of the organization, and time sensitivity of decisions. While one style is dominant with a leader, it is necessary to utilize varying approaches in different situations.

Autocratic leadership uses fear and coercion to achieve objectives. Within paramilitary organizations such as police or uniformed security forces, this style has a long tradition. It is

very directive in nature. It is most appropriate to use in emergency situations where decisions must be made quickly. It may also be appropriate with a new employee. Drill instructors and others in a training environment often bark out orders to their charges. This is appropriate on a firing range or when involved in some type of psychomotor skills training such as defensive tactics, crowd control, fire suppression, etc.

The autocratic style is usually not appropriate for continued usage. Over time, employees will resent this style. Autocratic management usually results in bored, unproductive employees who are resistant to change. Moreover, there may be informal groups formed within the workplace to restrict productivity (Huffmire and Holmes, 2006).

It must be emphasized, however, that autocratic leadership is not all bad. Sometimes the literature tends to give this impression, which is an oversimplification. Autocratic leadership is appropriate and necessary in certain settings. There is also a benevolent autocratic leadership style. This means that subordinates are commanded to do something. Afterward the leader explains why they made the decision to the subordinates in an attempt to gain their support.

Democratic leadership is participative. Democratic leaders solicit the opinions of subordinates in order to achieve objectives. Leaders present facts to subordinates. Subordinates are more like colleagues. Democratic leadership works well in situations that do not have serious time constraints and where the educational, training, and experience levels of employees are substantial. Investigative units and retail loss prevention departments are usually appropriate environments for a participative approach.

Of particular import is that a democratic leadership style may aid in maintaining an ethical workplace. As employees feel they can approach supervisors, they are more likely to seek direction involving ethical issues. They are also more prone to frank discussions about what they perceive to be wrong behavior.

Laissez-faire or "hands-off" leadership means that the manager or supervisor is simply not closely monitoring the behavior of subordinates. It may be best suited to those situations where subordinates are doing quite well on their own. It may also be appropriate in larger enterprises where it is simply impractical to be intimately involved in a supervisory role. Laissez-faire becomes problematic when it reaches extremes. In these cases it evolves into an absence of leadership. Managers who are "asleep at the wheel" cannot effectively steer the ship. Aside from operational inefficiency, there may be misconduct occurring with such a laissez-faire approach.

Women and Minorities

In modern America, it is foolish to expect that all, or even most, of our leaders will be upper-class white males. It is still more foolish to assume that a person's leadership ability is increased or decreased by his or her gender, racial background, religion, or sexual orientation. There is good reason why it is an illegal hiring practice to discriminate based on these characteristics: they have no bearing whatsoever on a person's ability to perform his or her job, be it the job of a line officer or the job of a supervisor.

In fact, there are many situations in which it is vital to have a diverse team of professionals.

Allan Pinkerton understood that female operatives were able to ferret out information in many instances where men could not. He employed the first female investigator, Kate Warne, in 1856. By 1860 there were several women on the payroll with Kate at their head. This was referred to by Allan as "my Female Detective Bureau" (Mackay, 1997, p. 74). This was fully 60 years before any American police departments had female officers.

Contemporary—and future—protection leaders may likewise benefit from a diverse workforce. For example, when it becomes necessary to search for weapons or contraband on the person of a female, it is advisable to have another female perform the search. When investigating a hate crime against a racial minority, a completely homogenous group of investigators may not be the best choice.

Diversity can begin at the top: a leader who is a woman or a member of a minority group can often benefit his or her team by offering a different perspective. This leads to increased awareness of, and sensitivity to, social issues that protection officers encounter on a daily basis.

The City of San Francisco offers several examples of competent female leaders in the public safety profession. Fire Chief Joanne Hayes-White was appointed to her position after only 14 years as a firefighter not only because of her skill, but also because of her "entrepreneurial approach," according to Mayor Gavin Newsom. This is an impressive accomplishment, especially for a woman in this traditionally male-dominated profession. Police Chief Heather Fong and District Attorney Kamala Harris are the first Asian–American and African–American women, respectively, to hold their offices. Their communication skills are championed throughout the city. These skills emanate all the way down to the line personnel that they lead. Mayor Newsom says, "I've often sat in envy of the ability of women to multitask, put ego aside, not complain, and solve the problem" (Breslau, 2005).

There are today many female executives and business owners in the security industry. A list of presidents of ASIS International reveals a number of women dating back over the years. Bonnie Michaelman, CPP, CHPA, was not only the 2001 ASIS President but also served previously as President of the International Association of Healthcare Security and Safety. Bonnie has also served on the Board of Directors of the IFPO and been involved in various academic initiatives within ASIS.

In spite of the need for and past record of achievement by them, women and minorities often face prejudice from customers and coworkers alike. Officers who refuse to accept a leader based on superficial characteristics such as race or gender have no place in today's workfo rce; however, some are still in the workplace and must be dealt with. There's a lot to be said for a woman or minority group member who steps up to the plate and leads his or her team effectively in spite of these additional challenges. Perhaps because of these obstacles, they often wind up being more prepared for leadership positions than our traditional white males.

Leadership in Crisis and Emergency Situations

Security professionals in both the public and private sectors have greater and greater roles to play in emergency and disaster management than ever before. The events of 9/11, serious natural disasters such as hurricanes and floods as well as economic catastrophes such as shortages of food, fuel, or electricity have propelled organizations to look at emergency management a lot more intently. A basic understanding of emergency management principles and practices is essential for continued career progression in the security industry.

The traditional, basic components of emergency management are mitigation, preparedness, response, and recovery (see Table 3).

Table 6.3 Basic Components of Emergency Management

Mitigation—sustained actions taken to reduce or eliminate risk. Mitigation activities focus on reducing either or both the probability of an emergency loss event or its consequence (degree of impact or criticality). Mitigation can be risk reduction or risk avoidance	Preparedness—a state of readiness to respond to an emergency or disaster. Human resources are ready to respond. Public education and training efforts are key aspects of preparedness. Resources necessary such as emergency equipment, medical supplies, food and water are stockpiled. So too is the protection of information
Response—recognizing and assessing the emergency. Setting up an alternate command, control, and communications center. Incident Command System has been developed for this purpose. Mobilizing resources necessary for dealing with the crisis is done at this juncture	Recovery—Recovery consists of a series of progressive steps; it occurs gradually, not immediately! The steps and resources necessary for their implementation must be identified in the planning process Traditionally many public and private emergency plans have neglected this phase of emergency management

During emergency situations effective leadership is essential at all levels of the protection organization. This is true during the initial response as well as when the subsequent steps toward recovery are being taken. Some key steps that leaders should take during emergencies include:

Be on the scene so that they can accurately assess the situation. Personal visits reduce the influence of subordinates or others "coloring" or "filtering" the assessment. This can be very important as some persons may be predisposed to "spin" things in a more positive light for any one of a number of reasons. Being on the scene also helps inspire confidence in others. Subordinates in particular look for a personal message from their superiors/leaders. Leaders who shake hands, hand out food and clothing after a disaster are more appreciated and effective.

Be informed. Many noteworthy leaders emphasized the importance of collecting and analyzing intelligence. During crisis situations information management is essential. Getting prompt, accurate "intel" is a challenge at times; but information guides decisions. New York Mayor Rudy Giuliani had an early warning system established a Syndromic Surveillance System to check daily with hospitals in order to identify elevated levels of disease symptoms. Data analysis done carefully could predict potential outbreaks. This enabled the City to supply extra personnel in the area of the anticipated outbreak (Giuliani and Kurson, 2002).

Keep employees and other stakeholders informed. There is a real need for constant and continuous communication during a crisis. Prior planning provides the opportunity to provide the maximum amount of information to employees ahead of the crisis. This includes conducting drills to test the effectiveness of the emergency plan (Woodward, 2005). Emergency operations centers at locations outside the affected area and redundant communications systems are necessary. Web sites with sidebars for emergency communication, ads in newspapers, television and radio announcements, and laminated cards with toll free numbers for employees to use in emergencies are all steps that can be taken to communicate.

Establishing liaison with other organizations. This may occur at virtually any level, from Director to Officer. During Hurricane Katrina, Loss Prevention Agent Trent Ward was the only person available from Wal-Mart in the city of Kenner, Louisiana. He partnered with a code enforcement officer from the City so that Wal-Mart and the city of Kenner could make decisions. Ward also worked with National Guard personnel, local police, and other retailers to ensure that food and water were made available to those in need (Trlica, 2005). The decisions and actions required in preparing for, responding to, and recovering from an emergency call for conduct "above and beyond the call of duty." Security personnel at all levels may have to assume roles above and beyond what the organizational chart calls for. The job description gets expanded. Rapidly! Managing emergencies makes a strong argument for broad-based professional development of protection staffs.

A classic shortfall in emergency planning is for organizations—particularly private companies—to plan as though they are the only entity affected. Plans must be made for area wide or regional disruptions in power, communications, etc. The need for interagency liaison here is obvious.

Being visible. In times of crisis, employees want to hear directly from their leaders. Former New York Mayor Rudolph Giuliani believed that attendance at funerals of City employees was essential, while going to a wedding was merely helpful. He had a saying: "weddings discretionary, funerals mandatory."

Being calm and setting the tone. Those who lead others must maintain their composure. They must also assess the situation and set the tempo of the response. Generally slowing things down a bit makes for calmness and better decisions. In some cases, however, a rapid, dramatic response is necessary. Those who lead must read the situation and perform according to its dictates in an exemplary manner: all eyes are on them!

Leaders in emergencies must model appropriate emotional behaviors. Expressing real, heartfelt emotions combined with a show of confidence and resolve is important (Mainiero and Gibson, 2003). When New York Mayor Rudolph Giuliani was asked by the news media how many casualties there were following the attacks on the World Trade Center on 9/11 he had no number. Experience told him that the media would hound him for an estimate. He replied "When we get the final number, it will be more than we can bear"(Giuiani and Kurson, 2002).

Learning what to say in public and to the media comes with training and experience. While dedicated media reps or Public Information Officers are essential, there may come a time when someone in a supervisory position must speak to the media. Persons who wish to progress in their careers would do well to craft their communications ability and learn as much as possible about media relations. This ability is important in marketing and crucial during emergencies.

Leadership Failures for Neophytes

An exploration of leadership in protection would be incomplete if some common failures were not identified. Sometimes seeing what does not work does a better job in explaining what does work than simply studying success. Of particular importance is the newly hired or promoted supervisor or manager—the neophyte. This is a critical juncture at which success or failure will be determined.

Carpenter (1995) provides a list of mistakes that newly appointed supervisors make:

1. Make changes immediately after being promoted. People generally resist change. Changes should be made judiciously after careful study of the situation.
2. Fail to develop "people skills."
3. Try to be "one of the guys." New supervisors must understand and maintain the appropriate distance between themselves and their subordinates.
4. Fail to delegate.
5. Are inconsistent in handling subordinates.
6. Do not talk to or listen to subordinates.
7. Fail to motivate their subordinates.
8. Fail to keep their supervisor informed. Bosses do not like surprises!
9. Make serious administrative errors due to failure to obtain sufficient information from management about what is expected of them.
10. Fail to effectively use their time. Time management is the key. Supervisors must supervise, coach, and mentor subordinates. At the same time they have administrative tasks such as payroll, scheduling, etc. They may also have investigative or other responsibilities.

At the higher levels of management, there are additional mistakes and problems that may confront the neophyte manager. Wells (2005) lists a set of pitfalls that newly hired executives may fall prey to:

1. Failure to establish key connections and build strong relationships. A new manager must "meet and greet" the important people around them if they expect to function at their fullest potential. Sitting in front of the computer screen is probably a waste of time early on in a managerial assignment.
2. Overconfidence. Some new managers think that they can immediately employ their old skills and experience in a new situation. This may not work in a new—and different—situation.
3. Significant, unexpected change where the new manager's job turns out to be different from what they initially anticipated. This may occur after receiving the "red carpet treatment" during the recruitment phase. There may also be a "honeymoon period "where things go quite amicably but then budgetary cutbacks occur."
4. Negative credibility. Sometimes there are negative perceptions of the manager. The manager must be careful not to engender this in any way. Negative perceived by stakeholders is very difficult to reverse. It is important to remember the old adage that:

   First Impressions Count.

Other leadership failures may occur either early on in an employment relationship or throughout the relationship. These include:

Failure to inspire often leads to project failure, incompletion, or even sabotage (Curtis and McBride, 2005).

Being defensive and insecure—being negative. Sometimes this may occur due to years of experience dealing with the lower classes in society. In others it may stem from the security organization being treated as the "illegitimate child" of the parent organization; the "black sheep." In these cases a dour perspective becomes a self-fulfilling prophesy.

Micromanagement. A frequently cited problem. Micromanagers look over everyone's shoulder and try and control everything (control freaks). They fail to delegate tasks and responsibility to subordinates. Micromanagers may be insecure. They may not be confident in their own worth and ability.

Adolph Hitler was a major micromanager. Having served as a corporal in the First World War he distrusted his own generals in the Second World War. He replaced many of them and turned the remaining ones into "Yes men" who only told him what they felt he wanted to hear. His lack of confidence in and support of his generals led to numerous military failures. He should have had a laissez-faire approach in many instances, allowing the generals to devise strategy for military operations and only overseeing the plans that were developed. Instead he overruled his generals and began leading Germany toward defeat. As a result Hitler's generals planned several assassination attempts against him.

There may be various reasons and interrelating factors in micromanagement. It is not a simple phenomenon. In security operations, micromanagement may stem from a negative, stereotypical view of security officers. This is a serious problem and managers must be on constant guard against it.

Huffmire and Holmes (2006) cite several reasons for managers being "control freaks":

1. It is anti-instinctive to delegate and a natural tendency to want to do the work oneself
2. A proclivity toward perfectionism resulting in a failure to trust others with one's work
3. An autocratic personality
4. Enjoyment in doing the work themselves
5. A failure in knowing how to avoid "upward delegation" that occurs when a subordinate comes to them with a problem; instead of helping the employee solve the problem they handle it themselves
6. A tendency toward being a "workaholic"

Failure to do homework on risk and the Return on Security Investment (ROSI). Contemporary managers in business and government seek quantitative analysis. They are focused on metrics. New York Police Commissioner William Bratton developed COMPSTAT in the early 1990s. This program provided a quantitative analysis of how police precincts were performing. Number of crimes were recorded and analyzed. The system also decentralized management and motivated police managers at the precinct level to produce more. What Bratton and his staff did in public policing is expected in a corporate environment. Effective security executives use PPM 2000, the CAPIndex, and various other tools to cost justify security programs. The need for empirical research in protection is greater than ever before; gone are the days of "seat of the pants" management where a director could state that "My 30 years in law enforcement have taught me that armed security officers deter robberies." Upper managers expect a quantitative analysis to be performed before funding any protection measures. They want metrics whereby each countermeasure must be researched from a deterrence perspective and costed out completely. There must be a systematic, monetary argument made for implementing protection measures. Security managers must then collaborate with other members of the organizational management team in order to quantify expenditures and expected ROSI.

While the above discussion relates to security program planning, the need for research in management is present in all situations. Managers must be prepared and meticulous. Presenting plans or budgets without having thoroughly thought them through leaves one open to attack. An old adage that all managers should be mindful of is:

If you don't do your homework—someone else will do it for you.

Cultural Misfits. It is essential when assuming a leadership position in a new organization that one respects the culture that already exists (Phillips, 1992). In security operations

culture is a major consideration. Unfortunately, some new leaders that are externally promoted may not understand, accept, or respect the organizational culture. These are often the "ex-something or others" who retire from police, government, or military careers and go into security management. Such a career transition may leave the new manager deficient in the physical applications and legal requirements of their new position—the technical aspects of the job. There is also an enormous cultural divide in many cases. The expectations of upper management and the various stakeholders are different than in their former careers. Protective planning is largely a matter of matching strategies and techniques to cultural environments. It is always a challenge to do this.

> *Security professionals must be part "Industrial Anthropologists" who study the culture of the protected environment.*

Not seeing or learning one's role in the organization. Persons promoted from supervisor to manager may be making a quantum leap in responsibilities. Sometimes this is part and parcel of the "cultural misfit/ex-something or other" syndrome. A lieutenant on a major police department who supervises a vast number of persons takes a job as a security director on a college campus. While the size of the staff may be smaller, there are now responsibilities to create and manage budgets, report to a higher level of management, etc. The result is a manager who is in "over his head."

Promotion is always a challenge. The type and degree of the challenge must be clearly understood by the employer, the person being considered for the promotion, and those within the new manager's work group.

Not seeing the protection role in the organization. A lack of vision concerning how security should be embedded within all departments. "Security is the grease in the machine; it touches all parts of the organization and makes it run more effectively." Protection of organizational assets creates an inherently "community-based" or "problem-oriented" environment.

Part and parcel of this issue is understanding the parent or client organization from a structural perspective. Knowing what the different departments are, how they function, and how they view their contribution to the larger enterprise is important. Disjointed management and lack of communication across departments result when this happens. Sometimes there is a duplication of effort between departments such as with IT and Security. Convergence between physical security, information security, and risk management is more productive. Managers with nonsecurity experience within the organization or specific industry (hospitality, healthcare, retail, etc.) may be better able to "talk the talk" and see "the big picture." They can more easily relate to the other members of the managerial team.

Supervisors within the organizations must have this vision. They should also ensure that it should be obtained by subordinates. New officers should be shown the organizational chart of the parent and/or client organization. They should understand where funding comes from and the limitations of budgets. As an example, shopping center security officers should understand that approximately US$130.00 per year is spent per square foot on security. Retail loss prevention personnel should understand the effect that shrinkage has on net profits. In public policing grant monies are often available from national and state or provincial governments. These are limited and have stipulations attached to them. Officers should understand this. Leaders must ensure that the officers understand and appreciate funding processes.

Conclusion

The many and varied leadership roles within security operations offer challenges and rewards. "Taking command" is essential for everyone in the protection business at one point or another.

Competent, career-oriented professionals have an extensive array of opportunities before them. This is particularly true in larger organizations. It is also true for entrepreneurial persons who wish to start or develop a small business. As threats and countermeasures continually evolve, so too must the responsibilities of protection professionals at all levels. Every person involved in providing security must learn and grow with the changing environment. Every one must lead.

Bibliography

L. Allen (1973). *Professional Management: New Concepts and Proven Practices*. New York, NY: McGraw-Hill.
K. Breslau (2005, October 24). A new team in town. *Newsweek* 146, 64–66.
J. Bullock, G. Haddow, D. Coppola, E. Ergin, L. Westerman, and S. Yeletaysi (2006). *Introduction to Homeland Security*. Burlington, MA: Elsevier, Butterworth-Heinemann.
H. Burstein (1996). *Security: A Management Perspective*. Englewood Cliffs, NJ: Prentice Hall.
M. Carpenter (1995). So you're a new supervisor. *Protection News* 11:3.
S. Covey (1989). *The Seven Habits of Highly Effective People: Restoring the Character Ethic*. New York, NY: Fireside.
G. Curtis and R. McBride (2005). *Proactive Security Administration*. Upper Saddle River, NJ: Pearson.
S. J. Davies and R. R. Minion (Eds.). (1999). *Security Supervision: Theory and Practice of Asset Protection*, 2nd edn. Burlington, MA: Elsevier Science.
G. Downing (2006). The balance of leadership. *Loss Prevention* 5(5):82–83.
G. Eastman and E. Eastman (1971). *Municipal Police Administration*. Washington, DC: International City Management Association.
E. Finneran (1981). *Security Supervision: A Handbook for Supervisors and Managers*. Woburn, MA: Butterworth.
K. Fitzgerald. *Sam Walton: The Model Manager of Wal-Mart*. http://www.stfrancis.edu/ba/ghkickul/stuwebs/bbios/biograph/walton1.htm; Accessed on December 2, 2006.
R. Fulton (1995). *Common Sense Leadership: A handbook for Success as a Leader*. Berkeley, CA: Ten Speed Press.
R. Giuliani and K. Kurson (2002). *Leadership*. New York, NY: Miramax.
M. Hammer and J. Champy (1993) *Reinventing the Corporation: A Manifesto For Business Revolution*. New York, NY: Harper Business.
S. Harowitz (2003) The New Centurions. *Security Management* 47(1):50–58.
C. A. Hertig (2004). *Principles of Supervision for First Line Supervisors*. York College of Pennsylvania, York, PA: Office of Community and Professional Development (Unpublished manuscript).
J. Horan and H. Swiggett (1951). *The Pinkerton Story*. New York, NY: Van Rees Press.
D. Huffmire and J. Holmes (2006). *Handbook of Effective Management: How to Manage or Supervise Strategically*. Westport, CT: Praeger.
V. A. Leonard and H. More (1978). *Police Organization and Management*. Mineola, NY: Foundation Press.
A. Longmire-Etheridge (2003). Getting down to business. *Security Management* 47(1):83–88.
J. Lucas (1988). *Command: A Historical Dictionary of Military Leaders*. New York, NY: Military Press.
J. Mackay (1997). *Allan Pinkerton: The First Private Eye*. New York, NY: John Wiley.
L. Mainiero and D. Gibson (2003). Managing employee trauma: Dealing with the emotional fallout from 9–11. *The Academy of Management Executive* 17(3):130–43.
L. McCreary (2006 January). *Women of Influence: An Awards Program Celebrating Female Infosecurity Achievement Recognizes a Quartet of Pioneers*. CSO Online. (http://www.csoonline.com/read/010106/women_influence.html; Accessed November 11, 2006).
N. D. Meyer (2005 July 26). *Mission, Vision and Values Statements*. CIO Magazine Online. http://www.cio.com/leadership/buzz/column.html?ID=9311; Accessed February 1, 2007.
W. Oliver and J. Hilgenberg (2006). *A History of Crime and Justice in America*. Boston, MA: Pearson.
P. J. Ortmeier (1999). *Public Safety and Private Security Administration*. Woburn, MA: Butterworth-Heinemann.
K. Peak (1993). *Policing America: Methods, Issues, Challenges*. Englewood Cliffs, NJ: Regents/Prentice Hall.
D. T. Phillips (1992). *Lincoln on Leadership: Executive Strategies for Tough Times*. New York, NY: Warner Books.

K. Poulin and C. Nemeth (2005). *Private Security and Public Safety: A Community-Based Approach*. Upper Saddle River, NJ: Pearson/Prentice Hall.
D. Slater (2004 February 17). *The ABC's of New Security Leadership*. CSO Online. http://www.csoonline.com/fundamentals/abc_leadership.html; Accessed on December 31, 2006.
C. Reith (1956). *A New Study of Police History*. Edinburgh, UK: Oliver & Boyd.
C. Sennewald (1985). *Effective Security Management*. Boston, MA: Butterworth.
N. Trautman (1993). Supervisory Ethics. In "*Supervisory Survival*," ed. E. Nowicki. Powers Lake, WI: Performance Dimensions Publishing.
J. Trlica (2005). He saved the city: One LP agent's experience in Katrina. *Loss Prevention* 4(6):28–30.
J. Trlica (2006). Lewis (Lew) C. Shealy. *Loss Prevention* 5(5):80–81.
R. Wadman and W. Allison (2004). *To Protect and to Serve: A History of Police in America*. Upper Saddle River, NJ: Pearson.
W. Weir (2005). *Turning Points in Military History*. New York, NY: Kensington.
S. Wells (2005). Diving in. *HR Magazine* 50 (3):54–59.
C. Wittmeyer (2003). The practice of management: timeless views and principles. *The Academy of Management Executive* 17(3):13–15.
N. Woodward (2005). Words to recover by. *HR Magazine* 50(12):52–56.
S. Zahra (2003). An interview with Peter Drucker. *The Academy of Management Executive* 17(3):9–12.
B. Zalud (2006). Security's 25 most influential. *Security* 43(12):28–47.

Leadership for Protection Professionals Quiz Questions

1. Management and leadership are synonymous terms; they mean the same thing.
   ☐ T ☐ F

2. An autocratic leadership style is inappropriate within contemporary police or security departments. ☐ T ☐ F

3. A well-known micromanager was _____
   a) Sam Walton
   b) Abraham Lincoln
   c) Adolph Hitler
   d) Alan Pinkerton
   e) Robert Peel

4. During emergencies, leaders need to keep employees and other _____ informed.

5. ROSI stands for:
   a) Refund On Software Inventory
   b) Return On Software Investment
   c) Return On Security Investment

6. The Thames River Police were a:
   a) Public police agency
   b) Private police agency
   c) Contract security agency
   d) Military organization
   e) Public–private partnership

7. The "father of police science" who believed in higher education for police officers in the early twentieth century was:
   a) Alan Pinkerton
   b) Robert Peel
   c) August Vollmer
   d) Patrick Colquhoun

8. A _____ statement says what an organizations stands for and whom it serves.
   a) mission
   b) vision
   c) values

9. _____ leadership may be needed when setting up a new security department, taking over a new operation or responding to a major organizational problem.
   a) Transactional
   b) Transformational
   c) Functional
   d) Operational

10. One who organizes, manages, and assumes the risks associated with running an organization is a() _____ leader.
    a) entrepreneurial
    b) inspirational
    c) visionary
    d) charismatic

UNIT VI

Risk Management and Emergency Management

This page intentionally left blank

1 Risk Management

Johnny May

Black's Law Dictionary defines risk as "the element of uncertainty in an undertaking; the possibility that actual future returns will deviate from expected returns." We encounter risks in every aspect of our daily lives. When we cross the street, accept a new job, or decide what type of automobile we are going to drive, we encounter some degree of risk.

Generally, when one mentions risk management, insurance immediately comes to mind. Risk management is a formal discipline—with its own jargon closely associated with technical, insurance, and legal questions. As such, it has developed a mystique that scares away the uninitiated.

Both loss prevention and risk management originated in the insurance industry. Fire insurance companies, soon after the Civil War, formed the National Board of Fire Underwriters, which was instrumental in reducing loss of property through prevention measures. Today, loss prevention has spread throughout the insurance industry and into the business community. Risk management is also an old practice. The modern history of risk management is said by many insurance experts to have begun in 1931 with the establishment of the insurance section of the American Management Association. The insurance section currently holds conferences and workshops for those employed in the insurance and risk management field.

There are five different types of risk with which organizations consistently have to deal:

1. Dynamic risks: Fluctuate under certain conditions such as weather or location.
2. Static risks: These remain constant without regard to other factors such as regulations, laws, or standards.
3. Inherent risks: These are unavoidable and are associated with a certain product, industry/business, location, and/or procedure.
4. Speculative risks: Occur when an organization initiates any new program, procedure, or operation. It also occurs when it enters into any activity, which might subject it to any other risk.
5. Pure risks: Natural disasters or criminal acts that do not fall into any of the above categories.

Source of Risks

- Human factors: Probably the greatest single source of risk, including both human error and failure.
- Mechanical factors: Are sources of risk resulting from any reliance on some type of machinery or equipment.
- Environment, crime risks, and civil disorders.
- Procedural factors: Are those sources of risk caused by the use of certain procedures, routines, or operation.

The goal of risk management is to design and implement plans to eliminate loss exposures, wherever possible, and to reduce to a practical minimum, the cost associated with those

losses that do occur. This entails using the risk management techniques of loss control and loss financing. The technique of loss control involves reducing the frequency and severity of loss occurrences, while loss financing addresses the minimization of the costs of those losses that do occur.

There are typically four types of losses to which organizations are subject:

1. Property losses: These types of losses most often come to mind when we think of loss prevention. Property losses involve buildings and their contents (furniture, office equipment, valuables, and proprietary information). Protection against property losses involves the reduction of hazards (fire, accidents, and crime) that cause loss.
2. Income losses: These losses arise when property involving income-producing activities such as stores, apartments, and other organization-owned facilities are subjected to some loss, which results in cessation of income produced by such property.
3. Legal liability losses: These arise out of duties owed by the organization to members of the society of which the organization is a part. Liability can arise out of statutory law, common law, and contract law.
4. Personnel losses: These result from the loss of services provided by any person in the organization who has a role in that organization's operations. When services individuals are lost due to illness or accident, the entire organization suffers a loss because these individuals are not available. Often, replacing these services can take place (through use of temporary agencies), but only at some additional expenditure of organizational funds.

Another good way to remember how losses occur is through the use of the acronym WAECUP (pronounced wake-up) which stands for Waste, Accident, Error, Crime, Unethical/Unprofessional Practices!

Risk management involves the identification and definition of specific problem areas and proper design of measures that will counteract the problem. Once a risk is identified, one or more of five specific methods can be selected to reduce exposure. These methods are:

- Risk avoidance: Risks can be avoided by taking the threatened object "out of harms way." This approach asks whether or not to avoid the risk.
- Risk transfer: The most common method of transferring risk in the business world is insurance. The risk manager works with an insurance company to tailor a coverage program for the risk.
- Risk abatement: Risks can be minimized to a level that is compatible with the daily operations of a business. Risks are not eliminated, but the severity of loss is reduced.
- Potential losses: Spreading the risk among multiple locations reduces risk spreading.
- Risk acceptance: Many business owners do this—they accept (or retain) risk as "part of the cost of doing business" without examining the alternatives available to them. Not every risk can be avoided, transferred, abated, or spread, but every effort should be made before a risk is accepted.

What does all of this have to do with security? One could say that a marriage of sorts exists between the risk manager and the security manager of a particular organization because of a common goal shared by both—protection of life and property.

The book "Suggested Preparation for Careers in Security/Loss Prevention" gives an excellent example (see below).

Suppose the following question was asked of two separate classes. One is a "security management" class and the other is across campus in the college of business and is in "principles of insurance." The question posed to both classes is as follows:

From the following job description you are to identify the person by job title, whose responsibilities within the corporation are as follows. Fill in the blank:

The primary and fundamental objective of the _____ manager is the preservation of assets and earning power from loss or destruction. He or she shall be responsible for identifying all exposures to such loss. The financial risk associated with each exposure to loss must

be evaluated as to both its severity and probability of occurrence. An action must then be taken to either eliminate said risks or reduce either the probability of their occurrence or the severity of their consequences. In summation, he/she is charged with preservation of the operating effectiveness of the corporation, by safeguarding both its assets and its potential income.

How do you suppose the two groups answered the question? You can bet the security class thought the job description was right out of their security book, and was describing the duties of the security manager. They would have filled the blank with the word "security". The business students, on the other hand, would have recognized that the description of duties fit risk management. Why? Well, one reason is that security is the counterpart of risk. The effective treatment of risks yields security. The two disciplines share some commonalities.

Another common interest shared by both risk management and security professionals is disaster planning. Both should focus on taking a proactive approach and formulating plans before tragedies strike. Then when the crisis arises, we need only implement the preconceived plan. An effective disaster plan could substantially reduce the economic impact of a catastrophic event.

Security also plays an important role in the overall risk management process. One of the primary sources of information available to the risk manager is the daily incident report generated by the security department. The reports give a brief description of unusual events that have recently occurred. Security is usually the first responder in the event of an accident, injury, or property damage. Incidents such as theft or vandalism are also reported.

The importance of these reports to the risk manager is obvious since they are his or her first indication that loss or potential for loss has occurred. Receipt of these reports enable the risk manager to provide an early response to the incident by putting all necessary legal, loss reporting (for insurance purpose) and loss control activities in motion.

Once a security professional reaches his or her ultimate goal, becoming the director of security, one may ask him/herself now what? Where do I go from here? How about risk management!

As one consultant notes, security people "often consider risk management to require a high level of involvement above and beyond the aspects and intelligence of security." And yet, says another, "a lot of security people don't realize they are already performing the risk management functions."

Assuming the position of risk manager usually means significant increase in responsibility and prestige, but it also means a similar increase in professional headaches as well. Yet, as one risk management consultant contends, "risk management is the natural goal for an aspiring security director … He or she already has the basic abilities of a risk manager. He/she uses the same principles.…{Security} programs revolve around problem identification and problem solving to eliminate hazards. You have to monitor your risk exposures and then try to minimize and reduce them. You do the same thing in risk management."

The risk manager's job varies with the company served. He or she may be responsible for insurance only; or for security, safety, and insurance; or for fire protection, safety, and insurance. One important consideration in the implementation of a risk management program is that the program must be explained in financial terms to top executives. Is the program cost-effective? Financial benefits and financial protection are primary expectations of top executives that the risk manager must consider during decision making.

Among the many activities of the risk manager are to develop specifications for insurance coverage wanted, meet with insurance company representatives, study various policies, and decide on the most appropriate coverage at the best possible price. Coverage may also be required by law or contract such as workers' compensation insurance and vehicle liability insurance. Plant equipment should be periodically reappraised in order to maintain adequate insurance coverage. Also, the changing value of buildings and other assets, as well as replacement costs, must be considered in the face of depreciation and inflation.

If one is interested in learning more about risk management, the Insurance Institute of America offers the Associate in Risk Management (ARM) designation. The program is designed for people whose careers include dealing in a cost-effective manner with exposure to accidental losses. Those who would benefit from the ARM program include corporate and

governmental risk managers, safety personnel, insurance producers and consultants, security directors, and insurance company commercial lines specialists.

The only requirement for earning the ARM designation is successful completion of three national ARM examinations administered by the Insurance Institute of America. The program consists of the following three risk management courses:

ARM 54—Essentials of Risk Management—focuses on the first two steps of the risk management decision-making process:

- identifying and analyzing the loss exposure
- developing alternative techniques for treating each exposure

It also introduces the student to the financial management foundation for the third step

- choosing the best risk management alternative, and explores guidelines for selecting the most appropriate technique for handling exposure

ARM 55—Essentials of Risk Control—focuses on the last three steps of the risk management process: selecting appropriate risk control techniques, implementing the chosen techniques, and monitoring the results for effective control and coordination of the organization's total risk management effort. It features further development and application of the guidelines for selecting risk management techniques introduced in ARM 54, especially in relation to the final steps of the risk management process.

ARM 56—Essentials of Risk Financing—finishes covering the risk management decision-making process with respect to risk financing techniques. Attention is directed primarily to various forms of risk retention and of commercial insurance.

For further information contact: Insurance Institution of America, 720 Providence Road, P.O. Box 3016, Melvern, PA 19355-0716.

Taking one insurance or risk management course will not suddenly transform a security supervisor into an expert. However, he/she may be surprised to find out that once they become familiar with even a small amount of the vocabulary and methods of the insurance industry, they become much more conversant with the insurance industry and with insurance professionals. Just being able to read and understand insurance requirements can make you a better security supervision.

Bibliography

J. Chuvala and R. J. Fischer *Suggested Preparation for Careers in Security/Loss Prevention*. Kendall-Hunt: Dubuque, IA.

P. Purpura (1991). *Security and Loss Prevention an Introduction*, 2nd ed. Butterworth-Heinemann: Stoneham, MA.

D. F. Shaffer (1993). *Public Safety Management Guide*, 2nd ed. Public Safety Management: Glenview, IL.

S. Taitz (1990). *Getting a Job, Getting Ahead, and Staying Ahead in Security Management*. Rusting Publications: Port Washington, NY.

US Small Business Administration (1994). Small Business Risk Management Guide.

Resources/Publication

Risk & Insurance, PO Box 980, Horsham, PA 19044; (2215) 784-0910
Risk Management, 655 3rd Ave, New York, NY 10017; (212) 286-9364
International Journal of Risk, Security, and Crime Prevention, Perpetuity Press, PO Box 376, Leicester, Le2 3zz, United Kingdom; +44 (0) 116 270 4186

Appendix A

Risk Management

A. Key Terms

Abatement Cost: "The cost of abating a nuisance such as pollution or congestion. In terms of pollution the cost curve will typically slope upwards at an increasing rate as pollution is progressively reduced. This is because it is usually comparatively cheap to 'clean up' some part of a polluted environment, but extremely expensive to remove the last units of pollution. An example would be noise where engines can be muffled, thus, reducing noise by a noticeable amount. Further reductions in noise, might, however, require expensive engine redesign or wholesale changes in road structures, locations, etc." Abatement cost would come from installing keypad locks on doors, which are protecting sensitive equipment. Abatement cost would be the total cost of installation.

Absorption: "1) In accounting, the process of factoring the cost of intermediate products and services into the total cost of the product. Absorption is also known as full costing. 2) In shipping, a gratis service provided by a carrier that is not covered by a published freight tariff or included in freight charges. Premium service includes free wharfage, switching, and so on. Depending on the law jurisdiction in which they are offered, premium services may constitute illegal inducement." Absorption comes when, during planning, a company decides to ignore a particular hazard, for example, a bomb threat. If a bomb is detonated, the company would absorb the costs to repair and replace damage assets.

Asset: Anything of value such as land, buildings, information, and image.

Business Continuity Planning: An all encompassing, "umbrella" term covering both disaster recovery planning and business operations following one of a number of disasters that might befall the business systems and resources. In this context, all business resources are considered, and services should not be confirmed.

Example: When your computer system shuts down, what system will you implement so as to continue with daily business, that is, phone calls, customers, and fulfilling orders?

Business Impact Analysis: To build a catalog of threats relating to the continued success of the business and to analyze the associated potential business impacts so as to define priorities for detailed analysis of vulnerabilities and implementation of controls. It is also the process of analyzing all business functions and the effects that a specific disaster may have upon them.

Example: What impact will a fire in a portion of your plant have on your productivity? What additional losses will you incur? Will you be able to function? If so, by what means and for how long?

Contingency Plan: A plan for emergency response, backup operations, and postdisaster recovery that the facility maintains as a part of its security program. A well-designed contingency plan provides many details about each step involved in preparing for, and responding to, an emergency. Although each plan differs in its details, contingency plans contain three major elements:

(a) Background Information
(b) Realistic Scenarios
(c) Response Actions/Countermeasures

Example: Being able to efficiently evacuate a crowded facility in the case of a bomb threat, fire, or natural disaster.

Countermeasures: Steps taken to combat the loss that has occurred.

Criticality: The impact of a loss as measured in dollars. Replacement costs, temporary replacement, "down time," discounted cash, and insurance rate charges are included as well.

Insurance: "Insurance permits individuals to exchange the risk of a large loss for the certainty of a small loss. The losses most commonly insured against are loss of property, life, and income. The purchase of insurance, by payment of an insurance premium, spreads the risk associated with any specified contingency over a large number of individuals. Insurance is said to be 'fair' if

the mathematical expectation of gain from purchasing the insurance is zeroed. The existence of administrative costs and any departures from perfect completion in the insurance market tend to make insurance less than fair, although this is frequently balanced by the tax treatment of insurance premia, and in practice insurance may be more than fair, i.e., the mathematical expectation of gain is positive." A company that purchases protection from fire knows that another company will pay for the losses incurred if there is a fire.

Management Generalist: This is a concept where the security manager has expertise in various aspects of management in addition to security. The security manager should attend staff meetings, listen to the problems and concerns of other managers, and try to help with his expertise.

Probability: Second step in risk analysis. It is essential to determine the probability of loss. The best way is to make subjective decisions about probability based on location and nature of the business.

Risk Assessment and Analysis: Management decision-making regarding loss control strategy, implementation of controls, and review of the effectiveness of these controls.

Risk Aversion: "The expectation of investors of a higher expected return as compensation for an increase in risk. A risk averter can be a diversifier and spread his portfolio over different assets, or a 'plunger' and invest wholly in bonds or money. A 'risk lover,' however, accepts a higher level of risk for a given expected return. If an individual is 'risk neutral' he would be indifferent between whether or not he accepted 'fair' insurance. Most individuals are generally held to be risk averters." Risk aversion occurs when a company outsources its security department. If an officer becomes injured due to negligence of those officers, he cannot sue the company, or file workers' compensation claims through the company because he was not hired directly by the company. In this manner, the company is practicing risk aversion.

Risk Management: "Also known as risk minimization, procedures adopted by an organization to reduce its exposure to potential losses. Banks sell commercial risk management services, including credit risk analyses, interest rate and exchange rate hedges, and business loan caps. In international trade transactions, banks and other firms determine country risk, based on evaluatitons of a specific transaction or the aggregate exposure in a particular country. Among others, risk minimization strategies include purchasing export credit insurance or overseas investment insurance, entering into barter arrangements, and requiring irrevocable letters of credit." Risk management occurs when a company purchases insurance, or hires and places patrol officers at access points, or purchases a CCTV system to observe a sensitive area.

ROI (Return on Investment): This term relates to cost-effectiveness. The business must get back what they put into the business. One formula for calculating ROI is ROI – ALE (old-ALE-(new) – C (cost for protective measure)).

Threat: These can be industrial disasters, natural disasters, civil disturbances, crime, and other risks.

Threat Assessment: The first step in risk analysis. You must identify the threats and vulnerabilities to the business.

Underwriters: Those who make up the insurance policies based on their experience of events in a certain area such as fires in certain types of businesses.

Vulnerability: Depends on the security posture, physical location, and the attractiveness of the assets to adversaries.

Being susceptible to abuse or misuse, or indiscriminate use; a weak point, soft spot, or a likelihood for error. In an automated system, situations that can compromise or neutralize a given piece of data or a security measure.

Example: A nation that does not account for, lockdown, and guard their national security documents is leaving itself vulnerable to a loss of classified records. This principle is applicable to most every entity and business.

B. Uses of Risk Management

1. Risk analysis shows the current security profile of the organization. It is diagnostic, showing management which areas need increased or decreased protection.

2. Risk analysis helps to compile facts necessary for the development of cost-effective safeguards through an examination of relevant threats.
3. Conducting a risk analysis can increase the security awareness of employees at various levels.
4. Can control, compile, and audit the cost of loss.
5. Can complement insurance protection in regards to lowering insurance premiums.
6. Security analysis can dictate procedural design for organization of a security force.
7. Through the use of different outside consultants you can gain differing perspectives on loss control within your organization.
8. Economic justification of expenditures with the security program
   (a) increased man hours
   (b) surveillance equipment (CCTV)
9. Recognition of vulnerabilities in all aspects of the organization and its security program.
10. Access risks and their possible impact on the organization.

C. Risk Management Process

1. Identify risk problems via a survey. The first step would be to make up an employee survey. This may not be totally accurate so you might want to study the employees with hidden cameras. By identifying our risks we should target the problems and try to correct or mitigate them. You might want to find the greatest area of weakness and which merchandise has the greatest threat.
2. Study the risks uncovered in the survey.
3. Collect information on probability, frequency, and criticality.
   (a) One way to collect information would be to study past incidences of loss.
   (b) There are many factors you must uncover and study when collecting information. You must find the Annual Loss Expectancy (ALE). To find this you must know the value of the assets in dollar amount (A) and you need to know the probability of how many times a year this might occur (L). You then multiply them together.
   (c) You also want to find Severity (S). There are two levels of this. The two are used to differentiate between a fire that destroys a whole building or a less damaging fire that started in a waste bucket.
   (d) Vulnerability to threat (V) also has two factors ranging from zero to one. It depends on how secure the asset is, the location and attractiveness of it. When calculating the ALE it is now more accurate: $ALE = A \times L \times S \times V$.
   (e) We can also calculate the ALE by multiplying the likelihood by the severity and the vulnerability ratings. This is called the Modified Likelihood: $ML = L \times S \times V$ or $ALE = A \times ML$.
   (f) After devising the new system from this information we have to calculate a modified ALE by multiplying the old ALE by 1 minus the effectiveness of the system: ALE (New) – ALE (Old) × (1 – E).
   (g) The Annual Cost© must also be found by making it equal to the sum of Depreciation (D) and the annual variable or Operating Cost (OC): C = D + OC.
4. Analyze various countermeasures:
   (a) Determine specific needs, risks, and vulnerabilities
   (b) Choose appropriate countermeasures:
      (i) satisfy needs, risks, and vulnerabilities
      (ii) cost effective—2% of the value of objects you are protecting
      (iii) ones which do not cause problems
   (c) Have interrelated parts that overlap whenever possible
   (d) Think in terms of the various responses to risk:
      (i) risk reduction—target hardening
      (ii) risk avoidance—"If you can't stand the heat, get out of the kitchen"
      (iii) risk transfer—let someone else be financially/legally liable

(iv) risk spreading—"don't put all your eggs in one basket"
(v) risk assumption—it is not worth worrying about or it can not be avoided

5. Implement countermeasures
   (a) Discreet placement without sacrificing effectiveness
   (b) Appropriate sites for alarms
   (c) Proper installation
6. Evaluate countermeasures
   (a) Test for effectiveness—can measures be improved?
   (b) Test under different conditions
      (i) weather—snow, rain, wind
      (ii) daytime and nighttime
      (iii) periods of heavy traffic
   (c) Test for durability

Appendix B

Source: *Risk Analysis and the Security Survey* by James Broder, Butterworth-Heinemann, 1984.

Frequency of Loss

Severity of loss	*High*	*Medium*	*Low*
High	Avoidance	Loss prevention and avoidance	Transfer via insurance
Medium	Avoidance and loss prevention	Loss prevention and transfer via insurance	Assumption and pooling
Low	Loss prevention	Loss prevention and assumption	Assumption

FIGURE 1 Decision matrix: A risk handling decision aid.

Appendix C

Source: *Introduction to Security*, 4th ed. by Gion Green and Robert Fischer, Butterworth-Heinemann, 1987.

	Probability		Criticality
(1)	Virtually certain	(A)	Fatal
(2)	Highly probable	(B)	Very serious
(3)	Moderately probable	(C)	Moderately serious
(4)	Probable	(D)	Serious
(5)	Improbable	(E)	Relatively unimportant
(6)	Probability unknown	(F)	Criticality unknown

Adapted from: Richard J. Healy and Timothy J. Walsh (1971). Industrial Security Management. New Yor American Management Association, p. 17.

FIGURE 2 Probability/criticality/vulnerability matrix.

Risk Management

Quiz

1. Generally, when one mentions risk management, _____ immediately comes to mind.

2. List the five different types of risk with which organizations consistently have to deal:
   a) _____
   b) _____
   c) _____
   d) _____
   e) _____

3. Both loss prevention and risk management originated in the finance business. ☐ T ☐ F

4. There are several different sources of risk which include: (Select incorrect answer)
   a) Human Factor
   b) Mechanical Factor
   c) Environmental Factor
   d) Procedural Factor
   e) Management Factor

5. The goal of risk management is to design and implement plans to eliminate loss exposures wherever possible and to reduce to a practical minimum the costs associated with those losses that do occur. ☐ T ☐ F

6. Define the acronym WAECUP:
   W _____
   A _____
   E _____
   C _____
   U _____
   P _____

7. Threat assessment is the first step in risk analysis. ☐ T ☐ F

8. List the four typical los ses to which organizations are subject:
   a) _____
   b) _____
   c) _____
   d) _____

9. Not all risks can be avoided, transferred, abated, or spread, but every effort should be made before a risk is accepted. ☐ T ☐ F

10. ROI is the acronym for:
    a) Risk Officer Individual
    b) Return on Investment
    c) Risk Orientated Individual
    d) Risk Officer Initiative

This page intentionally left blank

2

Why Accidents Happen: The Theories of Causation

Whitney D. Gunter

They're funny things, Accidents. You never have them till you're having them.
—Eeyore (from A. A. Milne's Winnie The Pooh)

Accidents occur everyday and, one way or another, will impact virtually everyone. During the year of 2005, there were approximately 4.2 million on-the-job nonfatal injuries in the United States (Bureau of Labor Statistics, 2006). That same year, there were also 5,702 on-the-job fatalities (Bureau of Labor Statistics, n.d.). Obviously, not all of these injuries are accidents (e.g., workplace violence and other nonaccidental injuries are included) but many of them are accidents. Additionally, on-the-job accidents account for only a small portion of injuries and fatalities following accidents. Further highlighting the impact of accidents is the costs absorbed by organizations. Even when workman's compensation is not a factor, employers often absorb costs relating to sick leave, health care, and, of course, time and money spent investigating the accident.

Even further expanding on the impact of accidents is the great number of accidents that do not result in injuries. In one of the earliest studies of accidents, H. W. Heinrich (1936) found that for every serious injury, there were 29 minor injuries and 300 accidents resulting in close calls. At that rate, even assuming that all injuries (major or otherwise) are included in the official statistics, there would be 42 million additional accidents that go unreported.

For the record, an accident is technically anything that happens by chance or misfortune. This definition provides two important points. First, accidents are unavoidable as a whole; the chance of one occurring will virtually always be present. Second, the chance of an accident occurring is a variable that can be changed. While it is impossible to prevent all accidents, it is possible to decrease their rate of occurrence. Understanding the cause of a phenomenon such as this is key to decreasing its occurrences, as often knowing the cause is the only way to formulate effective prevention strategies. Presented below are a few of the most common theories used to explain accidents. As with theories discussed in other chapters, these are not perfect and will not explain every accident in full detail. Rather, they provide a nomothetic explanation that seeks to explain what usually happens and attempts to address the most common underlying causes.

Heinrich's Domino Theory

As one can easily guess from the commonly used name for Heinrich's theory, Heinrich (1936) explained accidents using an analogy to dominos falling over one another and creating a chain of events. While this theory is not the most advanced or complex theory, it is especially noteworthy as one of the first scientific theories used to explain accidents. It is often still referenced today, seven decades later.

When dominos fall over, each tips the next enough to push it over and continue the process until all the connected dominos have fallen. However, if just a single domino is removed, the entire process ceases. Heinrich explains accident causation in the same way:

As you can see from Figure 2.1, Heinrich identified five stages of accident causation. The first stage, the social environment and ancestry, encompasses anything that may lead to producing undesirable traits in people. More precisely, this includes the nature and nurture aspects of someone's background. Genetics, poor parenting/socializing, and an unhealthy subculture are all examples of characteristics of nature and nurture that can negatively influence individuals and lead to the next stage of accident causation. It is worth noting that Heinrich's inclusion of genetics and ancestry is very much a product of the time it was written. A modernized version of this theory would likely use the term "inherited behavior," similar to how alcoholism and temperaments can be inherited. This stage of accident causation, especially the parenting and subculture aspects, is quite similar to the social learning theories discussed in the criminological theories chapter of this textbook.

The second stage, faults of a person, refers to personal characteristics that are conducive to accidents. For example, having a bad temper may lead to spontaneous outbursts and disregard for safety. Similarly, general recklessness can also be one of the manifestations of poor character. Ignorance, such as not knowing safety regulations or standard operating procedures, is also an example of this stage.

The third stage, an unsafe act or condition, is often the beginning of a specific incident. Unlike the first two stages, which affect the probability of accidents occurring, this stage is closer to the accident in terms of temporal proximity. This can include a specific act that is unsafe, such as starting a machine without proper warning, or failing to perform appropriate preventative actions, such as using guardrails or other safety measures. In essence, this stage entails acts (or failures to act) that occasionally cause accidents.

The next stage, logically, is the accident itself. This, in and of itself, needs little explanation. It is, simply, when something occurs that is undesirable and not intended. The final stage, injury, is the unfortunate outcome of some accidents. Whether an injury occurs during an accident is often a matter of chance and not always the outcome. This highlights the relationships between stages in terms of causality. An accident occurring is not a sufficient cause for an injury, but it is a necessary one. Similarly, the undesirable characteristics in stage two do not always occur in poor environments but could not occur without such environments.

Given this necessary causality, the most important policy implication is to remove one of the dominos (though try for more than one just to be safe)—produce a healthy subculture through positive accident prevention training and seminars, attempt to weed out people with undesirable characteristics (or otherwise address said traits), and, if all else fails, have a procedure in place for dealing with accidents to minimize injury and loss.

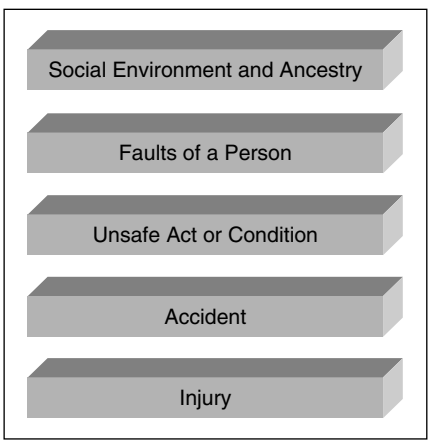


FIGURE 2.1 Heinrich's Domino Theory.

Ferrell's Human Factor Model

Unlike Heinrich, who explained accidents with a single chain reaction in vague terms, Ferrell's model incorporates multiple causes and is very specific about these causes (Heinrich, Petersen, & Roos, 1980). Additionally, Ferrell defines accidents in terms of being the result of an error by an individual. As such, he explains his theory using the assumption that accidents are caused by one person.

Ferrell identifies three general causes of accidents: overload, incompatibility, and improper activities. Each of these are actually broad categories that contain several more specific causes. Improper activities is perhaps the simplest of the concepts, as it encompasses two straightforward sources of accidents. First, it is possible that the responsible person simply did not know any better. Alternatively, he or she may have known that an accident may result from an action but deliberately chose to take that risk. The incompatibility cause is slightly more complex than improper activities. It encompasses both an incorrect response to a situation by an individual and subtle environmental characteristics, such as a work station that is incorrectly sized.

The remaining cause, overload, is the most complex of Ferrell's causes. It can be further broken down into three subcategories. First, the emotional state of the individual accounts for part of an overload. These states include conditions such as unmotivated and agitated. Second, the capacity refers to the individual's physical and educational background. Physical fitness, training, and even genetics play a part in this. Situational factors, such as exposure to drugs and pollutants, as well as job-related stressors and pressures, also affect one's capacity. Finally, the load of the individual can also contribute to an overload. This includes the difficulty of the task, the negative or positive effects of the environment (noise, distractions, etc.), and even the danger level of the task. Separate from each other, overload, incompatibility, and improper activities can all cause a human error to occur, which can lead to an accident.

Petersen's Accident/Incident Model

Petersen's model is largely an expansion on Ferrell's Human Factor Model (Heinrich, Petersen, & Roos, 1980). The notion of an overload, caused by capacity, state or load, is very similar to Ferrell's work. However, a few changes and refinements do exist. First, Petersen conceptualized the environmental aspect of incompatibility (work station design and displays/controls) as a different part of the model, calling them ergonomic traps. Additionally, Petersen also separated a decision to err from the overload cause. Further, Petersen also specified separate reasons to choose to err. These reasons include a logical decision due to the situation (primarily for financial cost and temporal deadlines), an unconscious desire to err (psychological failings), and perceived low probability of an accident occurring. The latter of these reasons, the perception of low accident probability, can include both actual instances of an accident being extremely unlikely and the natural inclination of a human to disregard his or her own mortality. This aspect of Petersen's model is akin to criminology's rational choice perspective (see the criminological theories chapter), as it makes the same assumptions of human rationality and hedonistic calculus.

Another noteworthy contribution is Petersen's recognition that human error is only part of a larger model. A system failure, the inability of the organization to correct errors, was added as a possible mediator between errors and accidents. These failures have a range of possible occurrences. The failure of management to detect mistakes and a lack of training are but two examples of systems failures. Even poor policy itself can lead to a systems failure that does not prevent an accident from occurring following a human error.

The Epidemiological Approach

Thus far, the chapter has focused on theories of accident causation. Each theory, while perhaps built on some anecdotal observations or one or two established relationships, is by definition highly theoretical. In other words, each is one person's best guess as to what is occurring. The

purpose is to explain some sort of correlation that has been observed (statistically or anecdotally). The Epidemiological Approach is different from these theories. Rather than take a little data and try to formulate a theory, the Epidemiological Approach continually relies on collecting additional information to expand our knowledge.

This technique can be observed in current insurance provider practices. For example, it could be observed that a company in one particular profession is more likely to experience an accident than the overall average. The insurance provider would then increase the insurance rates for any organization partaking in the more dangerous profession. The same type of experience could exist for a particular machine or even based on the geographic location. This can also show us what decreases the likelihood of accidents. For example, an insurance provider might observe that increased safety training programs are negatively correlated with accidents. Rates could be then lowered for organizations using such programs or a discount used as an incentive to increase training.

Systems Models

Most of the theories thus far discussed focus on human errors and environmental flaws. The Systems Model theory approaches the relationship between persons and their environments differently. Rather than the environment being full of hazards and a person being error prone, a Systems Model view sees a harmony between man, machine, and environment. Under normal circumstances, the chances of an accident are very low. Once someone or something disrupts this harmony by changing one of the components or the relationships between the three, the probability of an accident occurring increases substantially.

Another aspect of the Systems Model is what is referred to as risk-taking. Whenever someone chooses to do something, there is an associated risk (Firenze, 1978). Smaller tasks and risks are often calculated on an unconscious level. For example, when one chooses to drive to work each morning, that person weighs the risks (slight chance of being in a car accident) and the benefits (making a living) and decides the benefits outweigh the risks. This hedonistic calculus, as with Petersen's model, is quite similar to the rational choice perspective. Just as potential criminals may weigh the risks of being caught, managers, safety specialists, and supervisors consider the chances of injury or financial loss. The decision to move forward with the task is taken only when it is decided that the potential benefits outweigh the potential loss. In a real life example of this type of risk-taking behavior, Ford was once accused of deciding that the risks of releasing a defective vehicle (several fatalities that would result in wrongful deaths) were not enough to outweigh the benefit (not having to pay to fix all the defective vehicles). While subsequent reports have shown that this accusation is false to a large extent (Schwartz, 1991), this particular case has often been cited as an example of the ethical and financial calculations of risk-taking. Firenze (1978) suggests considering five calculated risks and benefits; see Figure 2.2. Additional information about these five factors becomes available through feedback after an initial attempt. In other words, a common task previously taken has well-known risks and benefits, while a new task often has more unknown factors.

1) Job requirements
2) The capabilities and limitations of the worker in relation to her or her job
3) The potential gain upon succeeding
4) The potential consequences upon failure
5) The potential loss of not attempting the task

FIGURE 2.2 Firenze's five calculated risks and benefits.

The Integration of Theories and General Program Implications

Much like other theories, each theory of accident causation does not explain every accident. Rather, each explains one possible cause of an accident. For example, the Epidemiological Approach fails to really explain why one thing causes an accident, just that it does. Heinrich's Domino Theory similarly fails to account for an environment, outside influences, or chance. Each theory explains only a portion of accidents and all of these theories are incomplete. It is therefore important to recognize that true accident prevention, the reduction of the probability of accidents, can occur only when all possible causes are addressed. Focusing on only one or two theories is simply not enough. Further, there are numerous theories not even briefly discussed in this chapter. Safety specialists and individuals with related duties are highly encouraged to consult additional information about accident causation.

There are numerous program implications that can be derived even from the few theories discussed in this chapter. Many of these are common sense, as they are often-used practices. First, most theories and models agree that human error is always a possible cause of accidents. One of the simplest ways to address this is to avoid hiring accident-prone or short-sighted staff and dismiss those who have shown carelessness. This, however, only addresses human error by eliminating the extreme examples (people who show carelessness even before being hired) or after an accident has already occurred. A more effective strategy is to train employees carefully. Only better safety training and increased knowledge of possible dangers can decrease the chance of an accident occurring.

Second, socialization and subculture are also a common thread in accident causation. This further underscores the need for regular training and safety programs. A poor employee not only increases the risk of causing an accident but also can corrupt future staff and make the problem grow exponentially. A safety awareness program is a good example of how to approach this problem. Regular meetings and positive safety posters are some of the tactics an awareness program can utilize. Keep employees motivated. The two-factor theory of motivation, also called the Motivator-Hygiene theory (Herzberg, Mausner & Snyderman, 1959), suggests that employees should be exposed to motivators (positive rewards) and hygiene factors (routine parts of a job, such as a good working environment, that prevent dissatisfaction). Management, whether involved in the awareness program or not, should also understand the importance of maintaining a positive subculture and be trained with intervention strategies for problem employees.

Third, the physical environment is also an important aspect of accident causation that must be addressed. In addition to obvious implications (guard rails, safety warnings, hardhats, etc.), the subtle relationships between man and machine must also be considered. Ergonomic designs, often used to increase productivity, can also increase a worker's comfort. Stress and boredom can play a role in human error, so keeping agitators to a minimum through ergonomic designs may also be helpful.

Finally, do not rely solely on conventional thinking. Being proactive and using outside-the-box thinking can improve a safety program substantially. Offering incentives and rewards to safety-oriented workers is a relatively new approach that, at a minimum, gets attention. The status quo can also be challenged by simply asking if more can be done. An important part of any program is an evaluation to make sure it is working. Statistical analyses of accident rates, surveys of individuals' perceptions of safety, and inspections by safety specialists are all examples of potential indicators of program effectiveness. Triangulation (confirmation) of the findings by using multiple indicators is important to validate findings. If possible, different programs should be implemented within different environments so that effectiveness (or lack thereof) can be compared. If a program is not working, ask how it could be made better. If it is working, ask the same.

Adapting Accident Causation to Specific Environments

Whenever a theory is developed for the social sciences, care must be taken to reinforce the purpose of such a theory. Unlike theories in the natural and physical sciences, sociological, business, and economic theories are often developed with a nomothetic goal. That is, these theories

are created in an attempt to explain most situations most of the time. They can neither account for all situations, as there will always be exceptions in the social sciences, nor can they provide the specifics of an explanation. Rather, accident causation theories, like other theories, are very general in nature. Developing specific policy implications from a general theory requires additional knowledge about the specific environment to which the theory will be applied. In other words, implications must be tailored to the needs and circumstances of an environment.

The aviation industry provides an excellent example of how the general theories and implications can be applied to specific industries. Here the primary concern of all accident theories, implications, and investigations is prevention (Wells, 1991). In addition to the obvious risk to human life in the event of an accident, the industry also has a public image that affects business and needs to be considered. One author observes, "accidents of the same type often require several different preventative measures" (Wells, 1991, p. 83). Therefore, the goal of accident causation theories and explanations in the aviation industry is to produce preventive measures even to the point being overly redundant. For this specific environment, the need for excessive prevention strategies outweighs the financial burden of such a tactic.

Industry-specific views of causality are also a consideration in aviation safety. In incident/accident investigations, the National Transportation Safety Board determines the causes of an accident in terms of a chain of causality and typically allows up to and including five specific causes in a single chain of events (Wells, 1991). This approach is quite similar to Heinrich's Domino Theory, yet is perhaps less specific about the nature of each domino. The safety programs also provide some insight to the application of theory to practice. In addition to the coordination efforts of air traffic safety and the high degree of training involved in flight, the aviation industry also has strict maintenance practices to reduce accidents. As noted in multiple theories, human error and machine failure are both potential causes of accidents.

In addition to the specific environment, one must also ask what type or types of accidents need to be prevented. For example, fire safety is a type of accident prevention that must be considered in virtually all environments. While the general theories of accident causation and the general implications from the theories certainly apply, more specific knowledge about fires and fire safety must also be considered. Most fire safety guidelines (e.g., Fiems & Hertig, 2001) include a discussion of the fire tetrahedron and how removing one of the causes of fire (oxygen, heat, fuel, or the chemical reaction) will prevent or stop a fire. This bears a striking resemblance to Heinrich's Domino Theory in which the prevention implication is to remove one of the dominos of accident causation. This serves as an illustration of how general theories can be applied to specific situations as well as specific environments.

The Future of Accidents and Accident Causation

Practical implications relating to accidents often have two parts. The main goal is obviously to prevent accidents, but since accidents can never be completely prevented, a secondary goal is to be prepared for the inevitable. On the reactive side of accidents, our path is vague. In the aftermath of the terrorist attacks of September 11, 2001, interest in emergency management has heightened. However, such interest has largely overlooked accidents, especially small accidents, in favor of terrorism and other malicious or intentional harm events (Haddow & Bullock, 2006). In the wake of Hurricane Katrina, the focus of emergency management has at least partially included nonmalicious events. Where does this leave the safety specialist concerned with small accidents and workplace safety?

Despite the lack of interest by the public and the media, accident prevention continues to be an important topic. Fiems and Hertig (2001) noted that fines by the Occupational Safety and Heath Administration (OSHA) have been increased and are being imposed more liberally than in years past for violations of unsafe working conditions. Additionally, more states are legislating safety standards and security organizations are placing more emphasis on providing both security and safety.

Since Heinrich's domino Theory in 1936, knowledge about accident causation and its counterpart, accident prevention, has grown remarkably. What once was the only theory explaining accidents has served as the foundation of a discipline home to many theories,

perspectives, and implications. This increase in knowledge, both among safety specialists and other individuals, has a substantial impact on safety in the modern world. Together with technological advances in safety and communication, accident causation theory and accident prevention are more advanced than ever before. Understanding and quantifying causation will lead us to a more scientific approach and cost-effective intervention strategies.

References

Bureau of Labor Statistics. (n.d.). Number of fatal work injuries, 1992–2005. Retrieved October 22, 2006, from: http://www.bls.gov/iif/oshwc/cfoi/cfch0004.pdf

Bureau of Labor Statistics. (2006). Workplace injuries and illnesses in 2005. Retrieved October 22, 2006, from: http://www.bls.gov/iif/oshwc/osh/os/osnr0025.txt

R. A. Fiems, and C. A. Hertig (2001). *Protection Office Guidebook*. Naples, FL: International Foundation for Protection Officers.

R. J. Firenze (1978). *The Process of Hazard Control*. New York: Kendall/Hunt.

G. D. Haddow and J. A. Bullock (2006). *Introduction to Emergency Management*, 2nd ed. Oxford: Butterworth-Heinemann.

H. W. Heinrich (1936). *Industrial Accident Prevention*. New York: McGraw Hill.

H. W. Heinrich, D. Petersen, and N. Roos (1980). *Industrial Accident Prevention*. New York: McGraw-Hill.

F. Herzberg, B. Mausner, and B. B. Snyderman (1959). *The Motivation to Work*. New York: John Wiley.

G. T. Schwartz (1991). "The myth of the Ford Pinto case." *Rutgers Law Review* 43: 1013–68.

A. Wells (1991). *Commercial Aviation Safety*. New York: McGraw Hill.

Quiz

1. For every serious injury, there are:
   a) 9 minor injuries and 90 close calls
   b) 29 minor injuries and 300 close calls
   c) 299 minor injuries and 9,000 close calls
   d) none of the above

2. Which of the following is not true of accidents in the United States?
   a) There are around 4.2 million on-the-job nonfatal injuries each year
   b) There are nearly 6,000 on-the-job fatalities each year
   c) There are very few on-the-job accidents that could be prevented
   d) There are potentially millions or billions more accidents that go unreported

3. According to Heinrich's Domino Theory, which of the following is not a cause of accidents?
   a) Faults of a person
   b) The social environment
   c) Sizable falling pillars
   d) An unsafe act or condition

4. Which of the following identifies overload, incompatibility, and improper activities as the primary causes of accidents?
   a) Heinrich's Domino Theory
   b) Ferrell's Human Factor Model
   c) Petersen's Accident/Incident Model
   d) The Epidemiological Approach
   e) Systems Model

5. Which of the following acknowledges that an individual or organization might choose to err?
   a) Heinrich's Domino Theory
   b) Ferrell's Human Factor Model
   c) Petersen's Accident/Incident Model
   d) The Epidemiological Approach
   e) Systems Model

6. Which of the following suggests considerations for taking calculated risks?
   a) Heinrich's Domino Theory
   b) Ferrell's Human Factor Model
   c) Petersen's Accident/Incident Model
   d) The Epidemiological Approach
   e) Systems Model

7. Which of the following seeks to explain accidents solely through statistical inference?
   a) Heinrich's Domino Theory
   b) Ferrell's Human Factor Model
   c) Petersen's Accident/Incident Model
   d) The Epidemiological Approach
   e) Systems Model

8. True or false?
   Focusing on a single theory is sufficient for a safety specialist to find implications.

9. Theories of accident causation can explain _____ situations _____ of the time.
   a) all, all
   b) all, most
   c) most, all
   d) most, most

10. True or false?
    Knowledge of the specific environment and specific types of accidents must be applied to the theories to obtain meaningful implications.

3 The Supervisor's Role in Safety

Randy W. Rowett and Christopher A. Hertig

Supervisors in security operations are often tasked with safety responsibilities. Whether or not this is one's primary area of expertise, safety is an important aspect of asset protection. Accidents can create extensive amount of loss. Accidents cause losses in the following areas:

1. Injuries to personnel. Sometimes these are life threatening; at other times they may cause protracted or permanent disability.
2. Damage to property and equipment.
3. An interruption in the work process.
4. Decreased morale among employees, visitors, customers, etc.
5. Costs of cleanup and investigation.
6. Potential penalties from regulatory agencies such as OSHA.
7. Possible civil actions being filed against the organization.

An additional concern is that safety ties in with fire protection. Generally when this is the case the term "life safety" is used. Fire is a tremendous problem because under the right conditions (sufficient heat and oxygen) almost anything is combustible. There are also safety concerns with smoke, toxic fumes, and explosions as a result of the fire. A fire event can cascade.

Emergencies require "prevention," "mitigation," "response," and "recovery" actions. So do accidents. A practitioner or academic with a solid background in safety is better able to navigate the demands of emergency management.

Industrial hygiene is a specialty dealing with health issues within safety. Prevention of epidemics and pandemics falls within the rubric of industrial hygiene. These are obviously significant for naturally occurring airborne or bloodborne pathogens. Certainly the efforts of industrial hygienists to prevent and control disease in the workplace tie in with response to weapons of mass destruction of the biological or radiological variety.

A foundation of knowledge in safety then can enable one to learn about other key areas. A solidly developed safety program will facilitate and support efforts to deal with related loss events. If the foundation is there, it is easier to adapt to fluid and varied risks.

Supervising Crisis Situations

Supervisors know that rarely do people call upon protection staff, or associate with them in most cases, unless in time of need or safety problems. This lack of contact can sometimes produce negative feelings, whereby protection staff feel as if they do not belong. Participation by security staff in local departments or facilities near the work area can assist in building relations and provide protection staff with the opportunity to contribute to the safety of the area or community through positive proactive functions.

Safety planning and the supervisory role is to set forth the correct response in crisis situations and to organize crisis intervention. As well, supervisors must recognize weaknesses and plan accordingly to achieve uniformity in critical areas.

No matter what type of crisis occurs, cooperation between protection staff and the public can be achieved by the following four steps:

a) Arrange safety meetings between key protection staff and supervisors.
b) Coordinate crisis plans through public relations/other departments.
c) Provide leadership and monitor all meetings.
d) Test the results.

When the correct formula for training is used, success will be achieved and a safety attitude will prevail.

Protection supervisors are tasked with a variety of functions relating to the safety integration of the public, customers, and employees.

Safety in the workplace requires that all personnel be trained in recognizing and rectifying problems before they occur. Examples of safety concerns where the supervisor is involved in training staff are fire safety, industrial equipment protection and use, unsafe work practices, health-related matters [first aid/cardiopulmonary resuscitation (CPR)], sanitation, hazardous materials, employee accidents and reduced injury plans, safety meetings, structural problems (which may cause injury or death), crime prevention, and many others.

Attitude plays a key part in safety approach development. Supervisors should be students of workplace socialization processes so that the correct attitude is developed. Some of the accident causation theories that discuss various aspects of workplace socialization are shown in Table 1.

Safety Committee Meetings

The safety meeting is more and more becoming a legislated and mandatory function in the workplace. Businesses suffering heavy costs and losses of work-hours due to injuries and illness caused by lack of protective equipment is another cost factor.

Safety committee meetings should include all sections or departments of a business. Naturally, security supervisors play a major role in participating in these meetings. Topics covered in these meetings are as follows:

a) Recent number of accidents per calendar month/year.
b) Number of employees injured/killed on the job.
c) Causes of accidents—tripping, falling, improper storage of items, improper safety shoes, malfunctioning safety equipment, structural problems of work areas, slipping on wet floors, insufficient safety training for employees, etc.
d) Steps to accident correction.

Table 1 Accident Causation Theories

Theory	Socialization Flaws
Heinrich's Domino Theory	The "social environment" teaches unsafe methods. Unhealthy values and behaviors develop within the work group.
Farrell's Human Factor Model	Improper activities are engaged in. These unsafe acts are performed because of simply not knowing any better or deliberate risk taking.
Peterson's Accident/Incident Model	A logical decision to err is made. This can be due to financial costs or deadlines. Another reason can be the perceived low probability of an accident occurring.

e) Illnesses caused by accidental or neglected industrial hazards.
f) Hidden cost of accidents (staff losses, replacements, and training of new employees).
g) Follow-up to results and problems.

As part of the safety approach development process, protection officers should participate in monthly inspections of facilities for accident prevention purposes. Conditions relating to health matters, such as unsanitary conditions and fire hazards, must also be reported. The security supervisor or manager then conveys these observations to the committee.

Safety Attitude Development

Security supervisors are responsible for the safety education of their officers. Every aspect of safety involves the need for awareness and prevention. The best way to meet that need is to introduce a learning process and safety practices.

There are many ways to start the safety program. For example, when an officer is first hired, incorporate a film on safety into the orientation program. The security supervisor should instruct new security staff and employees in other departments in the orientation program after hiring. This safety program should be attended by every employee and ideally should be a mandatory program for all new employees.

Methods by which to set up a safety attitude program are numerous and include the following:

a) Videos—there are many films on safety and prevention of accidents available from leading safety organizations.
b) Posters—messages such as "Accidents cost jobs and lives" are available from industrial safety companies and safety supply outlets.
c) Safety committee meetings—these will be discussed later.
d) Award programs—award employees who have made a solid contribution to the protection department in the interests of the safety program. Certificates can be created for such a purpose. Patches on uniforms can also be utilized. So too can stickers on vehicles.
e) Guest speakers/seminars by professionals—as a guest speaker for safety/security programs at business colleges, I can attest that students learn from and appreciate these seminars. In the workplace, they enhance learning development and employee morale.
f) Seminars that target people outside of the workplace such as family members of employees. Secondary or college students may also be potential markets. So too can groups of personnel that the organization wishes to recruit as employees. Providing an attractive certificate can be a powerful motivator for people to attend. The safety message gets out to the surrounding community as part of a community relations program.
g) For any company or organization that has a newsletter, there should be a security supervisor or director willing to write articles regarding local safety matters. Included in these can be crime prevention notes.
h) Websites and blogs can be used to communicate a safety message. These media have tremendous potential in terms of linkage to other sites, e-mails, posters, etc.

Make a list of potential means of communicating a safety message. Chances are there are some on the list that you did not think about and that could be exploited to great advantage.

The security supervisor must be familiar with all aspects of protection relating to safety. Part of this responsibility rests with the appropriate understanding, observation, and attitude toward existing or potential hazards.

Examples of safety matters are as follows:

a) Fire safety.
b) Industrial equipment protection and use.
c) Health-related safety (including first aid and stocking of materials, etc.).

d) Safe storage of hazardous materials and products.
e) Employee accidents and reduced injury plans.
f) Electrical hazards.
g) Structural problems (which may cause accidents or injury).
   i) Fire safety plans/disaster safety plans.
   ii) Ergonomic traps caused by improper work station design.and many others.

Safety in the workplace or in a facility requires that emergency personnel be trained in the recognition of potential problems before they occur. Prior emergency planning is effective in prevention of accidents. The use of "constructive daydreaming" by officers on post or patrol duty can identify potential accident scenarios. Attitude also plays a key part in safety development. Unsafe acts or improper activities are a major causal factor in accidents. These may be caused by the person not knowing any better or deliberately choosing risky behavior. Learn to recognize security hazards and correct them before they cause injuries or even death. Security and protection personnel can assist by watching for hazards such as

a) Blocked fire exits.
b) Improperly stocked shelves in cupboards or storage facilities.
c) Fire cabinets with improper or missing equipment.
d) Poor lighting in employee-traveled areas.

Supervising Accident Scenes

The protection supervisor is responsible for accurate and concise reporting and initial investigations of the accident scene. Regardless of whether an injury has occurred or whether it was narrowly avoided, the area must be sealed off and an investigation conducted to determine the cause. A review must then be made after the report has been submitted.

Remember the ten steps in supervising the reporting of accidents.

1. Seal off the area and notify emergency personnel (fire, ambulance, police, etc.).
2. Minimize risks to victims or bystanders (electrical wires down, fire, or gas leaks) and coordinate rescue, etc.
3. Treat victims for injuries (first aid/CPR).
4. Determine cause—that is, carelessness, vehicle accident, etc. Identify all causal factors rather than simply focusing on the primary factor.
5. Coordinate report—names of victims, addresses, liaison with emergency personnel attending, collect names, and badge numbers of workers, etc.
6. Follow-up with results of victim treatment and assign trained safety investigators. (Police investigations will take priority; however, internal investigation can be conducted.)
7. Interview witnesses.
8. Final examination—determine if the follow up removed existing hazards from scene (to prevent a second incident).
9. Collect all information for presentation to safety committee and outside agencies.
10. Review matter with safety committee.

When a person commits himself or herself to the task of security, protection, or law enforcement work, there is an understanding that we may encounter danger through risks of injury or even death while performing our duties. We also know that, as supervisors, we need to be aware of constant inherent dangers caused by risks such as fire, bombs, assaults, and domestic disturbances.

The supervisor who has been on the job for any length of time must be prepared for any eventuality and coordinate training for the protection of his or her staff. These planned training sessions not only involve physical response but also emotional control and remedial response in an approved professional manner. Safety relates to staff in a variety of work-related problems. Some protection staff may be in need of supervisory advice, and supervisors should be familiar with employee assistance programs. Stress-related factors can cause

carelessness in decision making. Farrell's Human Factor Model refers to this as "overload." Organizational safety development should provide for the handling of stress and pressure on the job. The supervisor should be ultimately prepared to intervene if there is a risk of injury to officers or the public due to work/personal problems.

The second rule to safety approach development for the supervisor is, "Be available to address safety concerns." These concerns can be established and created from any person or source. Peterson noted that a system failure by management to correct problems was a mediator between errors and accidents. Supervisors need to serve as "auditors" of safety systems who can detect flaws and take the appropriate action to correct them.

Enforcement of Safety Regulations

The security supervisor is part of the management team. It is therefore the supervisor's responsibility to monitor and ensure that all safety regulations are being maintained in compliance with policy.

When violations occur, investigations must be initiated and corrective action taken to correct any fault in the safety protection plan.

Types of safety regulations to enforce include the following:

a) Fire safety—trash, papers, nonsmoking areas, etc.
b) Malfunctioning or missing protective safety equipment—abuse or failing to wear appropriate devices.
c) Workers using unsafe practices—this action can lead to employee injury or injury to bystanders. Another example is staff going into risky areas without proper back up from officers.
d) Nonalert staff—part of the problem may be staff shortages causing fatigue due to extended hours. This is a risk situation. Extra long hours diminish capability and concentration. Proper sleep, diet, and lifestyles assist in an alert staff. Frequent breaks can also help reduce inattention and the resultant errors in judgment. So do the removal of distractions (lights, noise) from the environment.
e) Health/Sanitation—security officers should be instructed to report unhealthy practices relating to risk. An example is unsafe food handling. Food-related illnesses can cause extensive sickness within an environment. They also create negative publicity.

There are many other areas to be considered. One point of importance is the compliance factor. Security staff must enforce and also comply with existing policies and regulations. Security supervisors have a required duty to assist in monitoring compliance to safety matters. One rule to remember is, "If you enforce the safety rule—do not violate it!"

Types of Conduct/Violations Causing Accidents

- Blocked fire exits or insufficient equipment.
- Electrical problems.
- Chemical storage (flammable) violations.
- Improper lighting.
- Lack of fire equipment.
- Training insufficiencies—safety policies.
- Employee carelessness.
- Insufficient surveillance equipment.
- Lack of awareness.
- Ego errors or faults of a person such as being bad tempered or reckless.

Natural Causes of Accidents

- Aircraft incidents.
- Earthquakes.
- Floods.

- Wind damage.
- Fires due to lightning.
- Power outages—electrical.

Corrective/Proactive Approach

- Frequent inspections—measuring results.
- Set up guidelines and policy retraining.
- Ensure all equipment (at least minimum acceptable standard) present.
- Arrange security/safety awareness program.
- Provide first aid, CPR, and rescue training.
- Coordinate with local authorities.
- Ensure all mechanical equipment functions.
- Annual retraining, testing with safety programs.
- Bring in experts in the field, instructors of safety programs.
- Crime prevention activities.

Fire Safety Supervisory Functions

The following tips are useful for allowing protection supervisors to coordinate, develop, and maintain fire safety programs.

- Know types of fire extinguishers to be used. Do not rely on a specific department in a facility to handle situations entirely. Supervisors must train protection officers and facilitate professional liaison with government safety inspectors and law enforcement persons. Therefore a good supervisor will always learn and practice as much about fire safety as is required. Certain fire codes must always be maintained and knowledge of these codes is essential. Check with your local fire department or fire prevention company for courses and information pertaining to codes, prevention, and enforcement. Make certain that municipal, state, and provincial code compliance is maintained.
- Coordinate plans for emergency response. Liaise with fire department personnel. Have a meeting with authorities near an airport, sporting facility, or major business. Develop evacuation plans and initiate a plan to share shelter and aid with other organizations in the event of an emergency.
- Train security or protection personnel in types of fires, types of extinguishing materials, and causes of fires. Develop proposals for fire protection such as cameras, flame detectors, heat sensors, smoke detectors, and ionization detectors. This is useful for both fire safety and regular security duties.
- Introduce and utilize crash carts in every facility. Included should be oxygen, first aid kits, extinguishers, smoke masks, flashlights, and any other items required.
- Organize inspections by protection staff on a monthly basis. Any facility or property will benefit from this proactive approach to fire safety.

Protection supervisors have key responsibilities for ensuring the success of safety programs. The following is a list of pertinent duties.

a) Coordination at local command post of accident.
b) Policy formulation and awareness programs.
c) Reviewing accident statistics and corrective approaches to lower accident numbers.
d) Officer safety training and safe response practices.
e) Implementing first aid/CPR programs.
f) Investigation of actual and observed safety hazards through inspections.
g) Liaison with local authorities and businesses.
h) Ensuring all pertinent investigative material is available for local authorities, court, or insurance matters. Supervisor must be aware of company or organization regulations pertaining to reporting and command chain of same.

i) Lists of on-call personnel to dispatch in the event of an emergency. Security staff must have personal phone numbers at the department for call-out purposes.
j) Arrange awards for outstanding safety contributions.
k) Organize and supervise awareness campaigns such as crime prevention, accident watch, and many others.

Summary

This chapter has been a brief examination of safety. The emphasis is on observation, prevention, attitude, and approach to various problems and procedures. Throughout any organization there are accidents that are tragic in nature. Some are caused by wrongful acts such as crime or negligence. Many more are caused by weaknesses in observation and reporting as well as correction; some accidents still happen because of improper attitude and improper approach to the situation. Any supervisor, whether experienced or a career protection officer wishing to advance to a supervisor position, to set up the best protection program possible. Include in this program items related to safety. Integrate safety inspections, crime prevention, equipment usage and protection, committee meetings, employee participation, and safe work practices. Each initiative has some degree of overlap and carryover with other areas.

The protection supervisor is tasked with all these duties and more. If you have ever investigated accidents, and knew these were preventable (at less cost to the company, less loss of worker hours due to injury, and terrible records for safety), you as a security supervisor owe it to the department to create a rewarding safety protection plan for the benefit of everyone. The rewards for promoting safety are ongoing. We all chose to work in the protection field. Let us strive to make things as safe as possible.

Quiz

1. When the correct formula for _____ is used, success will be achieved and a safety attitude will prevail.
2. Every aspect of safety involves the need for _____ and prevention.
3. Prior emergency _____ is effective in prevention of accidents.
4. Security staff must _____ and regulations.
5. Organize and supervise _____ campaigns such as crime prevention and accident watch.
6. As long as there are some maintenance people on duty in a facility, the supervisor can rely on this experience for full fire protection with minimal involvement in the process. ☐ T ☐ F
7. It is not necessary for security staff to respond to power outage situations. ☐ T ☐ F
8. Supervisors should ensure that only water-based types of extinguishers are available for firefighting in work areas. ☐ T ☐ F
9. A crime prevention program focusing on offensive prevention is part of the safety awareness program. ☐ T ☐ F
10. Staffing considerations are of little factor in implementations of safety approach development. ☐ T ☐ F

This page intentionally left blank

4 Workplace Violence

Inge Sebyan Black and David A. Black

Security professionals now identify workplace violence as one of the most significant security concerns, even greater than fraud, terrorism, Internet/Intranet security, emergencies, embezzlement, and other security-related issues. This is an ongoing problem in today's work environment and it has a significant impact on businesses, both financially and morally. Employers have a legal and moral obligation, along with the responsibility to provide a safe and secure work environment. Every day thousands of employees are subjected to workplace violence. One might think of violence as a physical assault. Workplace violence is actually much broader. It includes threatening behavior, harassment, veiled threats, intimidation, and verbal or written threats or physical attacks. It also includes anger-related incidents, rape, arson, property damage, vandalism, and theft. Incidences can occur at off-site business-related functions like conferences, trade shows, social events, or meetings but we refer to it as workplace violence because it takes place at work.

Violence is so prevalent in the workplace today that the Centers for Disease Control and Prevention have labeled it "a national disease epidemic." It is important to note that individuals who work with the public are at much greater risk from the public than they are from coworkers; however, for the purpose of this chapter we are focusing on coworkers, disgruntled employees, and domestic issues.

According to OSHA (Occupational Safety and Health Administration) the most extreme form of workplace violence, homicide, is the fourth-leading cause of fatal occupational injury in the United States. There are currently no specific Federal OSHA standards to address workplace violence. Section 18 of the Occupational Safety and Health Act of 1970 (the ACT) encourages States to develop and operate their own job safety and health programs. OSHA approves and monitors State plans. There are currently 24 states; Puerto Rico and the Virgin Islands have OSHA-approved State Plans and have adopted their own standards and enforcement policies. For the most part, these States adopt standards that are identical to Federal OSHA. However, some States have adopted different standards applicable to this topic or may have different enforcement policies. In Section 5(a)(1) in the "ACT," it states that "each employer shall furnish to each of his employees employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees." In a workplace where the risk of violence and serious personal injury are significant enough to be "recognized hazards," the general duty clause would require the employer to take feasible steps to minimize those risks. Failure of an employer to implement feasible means of abatement of these hazards could result in the finding of an OSHA Act violation.

If we are to combat violence, we need to understand the magnitude, identify potential aggressors and victims, and identify viable solutions to protect our organizations from this violence.

Workplace violence is such a complex issue because it is not possible to isolate any one factor; there are so many psychological and physical factors that may force an individual into committing a violent act. Every individual reacts differently to stress which makes determining exact causes difficult if not impossible. There are proactive steps companies can take that will make them better prepared to handle any situation.

This chapter will first address the critical components of what every business needs to consider in order to effectively address workplace violence. We will then look at assessing general risks along with the assessment of a reported specific threat. We will look at strategies for mitigating risk and procedures and policies adequately.

The Basics

The following are some suggestions on best practices for a workplace violence program; however, it is the opinion of the authors that to be successful in implementing any workplace violence program, it is crucial that you first have the commitment of management.

- Implementation of a reporting system in which employees are encouraged to communicate concerns
- Creation of a threat assessment team which should include Corporate Security, Human Resources, Legal, Facility Management, EAP, Immediate Supervisory Personnel, Union Representative (if necessary), and, in some instances, Police Liaison, Medical/Psychological expertise
- A workplace violence prevention policy
- Specific prevention strategies should be publicized company-wide
- Appropriate training sessions, including training all supervisors in nonviolent conflict resolution
- The success and appropriateness of intervention strategies should be monitored and adjusted with continued data collection
- Management commitment is best communicated in a written policy. The policy must:
  - Be developed by management and employee representatives. Company officials, security managers, and representatives from all areas of the firm should serve on a committee to study workplace violence
  - Apply to management, employees, clients, independent contractors, and anyone who has a relationship with your company
  - Define what you mean by workplace violence in precise, concrete language and then communicate this
  - Provide clear examples of unacceptable behavior and working conditions
  - State in clear terms your organization's view toward workplace violence and its commitment to the prevention of workplace violence
  - Precisely state the consequences of making threats or committing violent acts
  - Outline the process by which preventive measures will be developed
  - Encourage reporting of all incidents of violence
  - Outline the confidential process by which employees can report incidents and to whom.
  - Assure that no reprisals will be made against reporting employees
  - Outline the procedures for investigating and resolving complaints
- Make a commitment to provide support services to victims of violence
- Describe how information about potential risks of violence will be communicated to employees
- Offer a confidential Employee Assistance Program (EAP) to allow employees with personal problems to seek help
- Make a commitment to fulfill the violence prevention training needs of different levels of personnel within the organization
- Make a commitment to monitor and regularly review the policy
- State all applicable regulatory requirements
- Perform a thorough threat assessment

Assessing the Risk

General Risk Assessment

Security experts look at a variety of data to help assess the risk. This data is essential for assessing the nature and magnitude of workplace violence in the particular workplace. It helps

to quantify the risk. The data collected helps assess the need for action which helps reduce or mitigate the risk. It is from the assessment that you can implement a reasonable intervention strategy.

- Conduct a visual inspection of the workplace and the type of work being done. Focus on the workplace design and layout. Review the administration, corporate culture, and work practices.
- Review and determine whether your workplace has any of the risk factors associated with violence. Is your business targeted for terrorism, animal rights activists, or antiabortion activists? Additional factors include a history of violence, present employee issues, past employees, known domestic issues involving employees, disturbing behavior, chemical dependency issues, and elevated frustration by employee with environment, personality disorders, or romantic obsession. By consulting existing incident reports, committee records, and having conversations with human resources, facility management and other employees, you can gain a sense of what risk might exist now or in the future. Identify environmental risk factors, geographical risk factors, and physical risk factors. If you do not yet have a system to document historical violent incidents, this should be done. Research any incidents that might have been reported to law enforcement.
- Interview employees. A workplace violence committee or taskforce, once in place, should consider conducting interviews, which can be both in person and through online surveys.
- Identify other same/similar places of employment and review their history and strategies they have implemented. Obtain information from any umbrella organizations with which you are associated; for example, your industry association, workers' compensation board, occupational health and safety regulators, or union office.

Organize and review the information you have collected. Record the results of your assessment. Use this document to develop a prevention program with specific recommendations for reducing the risk of violence within your workplace. Do your customers provide a higher risk? Are your employees planning a strike?

Threat Specific Assessment

Initial Steps

1. Corporate Security should conduct an immediate investigation and interview the witnesses/complainants and the subject.
2. If the situation has not been resolved at this point, the threat assessment team should convene immediately and a thorough assessment should be made. Each member of the team will have specific responsibilities to ensure the safety of all concerned.
3. If the threat is deemed serious and violent actions appear imminent or likely, an increased security stance should be adapted.
4. If the facility has no external security such as a guard house or locked doors, security should be enhanced. It is strongly advised that all who may be first encountered by an aggressor, such as the receptionist, be fully aware of threats and be knowledgeable about procedures. Appropriate individuals should be provided a photo of the subject.
5. Police emergency response personnel should be invited to tour the facility and provided with blue prints.
6. Individuals likely to be targeted by an aggressor should have the option of fleeing to "a safe room," otherwise known as a panic room. All emergency personnel should be familiar with this location.

Follow-Up

1. In consultation with legal and law enforcement, consideration should be made in pursuing criminal charges.
2. If criminal charges are not appropriate, then determine the feasibility of a restraining order.

3. Direct, discreet surveillance of the subject(s) should be thoroughly assessed before implementation. This may prevent or warn of an attack but could also instigate one if surveillance is detected.

Many executives feel threatened at their homes but keep in mind workplace violence so named for a reason. Attacks at executive's homes are virtually unheard of.

4. Individuals likely to be targeted should be assured that everything possible is being done to protect them, and specific security training should be offered to teach such things as changing their routine, changing their parking, and mode of transportation. Carpooling or availability of an escort to and from work should be discussed.

Awareness Through Training and Experience

As Security Professionals, we need to be aware of employees that might be of greater risk. Supervisors should be trained to understand and take seriously threats of physical violence or statements about revenge. In almost all cases attacks are perpetrated by individuals who display some of the following characteristics but there is a trigger that causes someone to act out.

- Prior history of violence: Involvement in previous incidents of violence, verbal abuse, antisocial activities
- Domestic/personal situations: An employee caught in a domestic dispute or family turmoil which may impact the work place
- Mental disorders: Mood swings, depression, bizarre statements, paranoid behavior, unusually irritable, overly aggressive, unstable behavior
- Life-changing events: Whether the employee has suddenly lost a family member, a pet, extreme medical changes or divorce, major life changes
- Financial stresses such as bankruptcies, mortgage arrears, or heavy debt load
- Obsession with another employee: May be romantic or not
- Chemical dependence: Drugs or alcohol abuse
- Increased interest in weapons: Ownership of guns or gun collection, other offensive weapons
- Disgruntled employee: An employee feels the company no longer cares about their employees creating a sense of mistrust

A Safer Workplace

Forming a workplace violence threat assessment team was one of the recommendations listed above. This team might consider implementing some of these steps:

- Hiring and retention practices: This involves conducting a comprehensive background and reference check on all new employees, including drug screening. It also involves consistent discipline practices.
- Proper supervision: Properly train supervisors on behavioral warning signs.
- A zero-tolerance policy: In your workplace violence manual, provide a clear definition of what the company considers violent behavior and the penalties for violating the policy.
- Investigate and take serious all reports. Proper documentation is one of the best ways to protect yourself and your company should litigation arise.
- Take action under a violence prevention plan if a viable threat of violence is present.
- Develop a disaster recovery plan. It should include provisions such as counseling and time off.

Bibliography

National Institute for Occupational Safety and Health (1996). *Violence in the Workplace: Risk Factors and Prevention Strategies*.

BWC: Division of Safety and Hygiene, Violence in the Workplace, Revised 2002.
Violence in the Workplace: A Prevention and Management Guide for Businesses, By S. Anthony Baron, PhD.

Workplace Violence

Quiz

1. Employers have a responsibility to provide a safe and secure work environment? ☐ T ☐ F
2. Workplace violence is a complex issue? ☐ T ☐ F
3. You can put together a plan for a workplace violence program without buy in from management. ☐ T ☐ F
4. An EAP (Employee Assistance Program) is a confidential way that employees can seek help with personal problems. ☐ T ☐ F
5. Collecting, reviewing, and organizing information that you collect when assessing the workplace for risks of violence is extremely important in reducing the risk ☐ T ☐ F
6. Employees such as a receptionist should never be informed of a potential risk for confidentiality reasons. ☐ T ☐ F
7. Employees with a prior history of violence may be one indication of a potential problem. ☐ T ☐ F
8. Mental disorders, financial problems, divorce, family death, or an increased interest in weapons are several indicators of a higher risk for violence. ☐ T ☐ F
9. All reports of violence should be taken seriously. ☐ T ☐ F
10. Having a violence prevention plan is the first step in providing a safer workplace. ☐ T ☐ F

This page intentionally left blank

5 Critical Incident Management in the Post-9/11 Era

Ernest G. Vendrell and Scott A. Watson

Introduction

In the post-9/11 era, it has become increasingly fashionable for security professionals to discuss how the disciplines of physical security and information technology are converging and thus changing the very nature of protective services. While these discussions are both important and positive, they fail to fully address the rapidly shifting nature of today's security threats. The central reality of security in the post-9/11 world is that the complex nature of critical incidents necessitates an interdisciplinary response.

Security professionals must be prepared to deal with a wide variety of critical incidents including crime, weather-related emergencies, cyber-attacks, terrorism, product tampering, and a whole host of other issues. In order to adequately respond to today's critical incidents, today's security professionals must have an understanding of not only traditional security disciplines and information technology but also general business practices, risk management, crisis management, business continuity, disaster recovery, and public safety to name just a few. Convergence is indeed coming, but it is much grander than what is encompassed in the current discourse. (CSO Magazine, 2007, www.csoonline.com/fundamentals/abc_convergence.html)

The words of Benjamin Franklin at the signing of the Declaration of Independence ring as true for security professionals today as they did for the founding fathers in 1776: "We must all hang together, or assuredly we shall all hang separately."

Most experts today are predicting that corporations, businesses, law enforcement agencies, as well as various other governmental entities in the United States and around the world will be confronted with critical incidents that are likely to increase in number and level of severity (Sylves and Waugh, 1996; Paschall, 1992; Gigliotti and Jason, 1991). As a result, planning for critical incidents has taken on greater importance as well as a renewed sense of urgency.

Critical incidents are unplanned events such as natural disasters, hazardous materials spills, transportation disasters, terrorism, workplace violence situations, and other similar life-threatening events. The extraordinary dimensions of these situations require special organizational skills and abilities on the part of emergency response personnel in order to attain a successful outcome.

Consequently, an emergency response plan that provides the necessary structure for managing critical incidents is of vital importance to any organization. Besides helping to save lives and reduce property loss, a well thought out emergency response plan can serve to lessen an organization's potential liability. Developing a comprehensive emergency response plan is, therefore, one of the most essential functions that a security supervisor or manager can perform.

Scope of the Problem

Unfortunately, many organizations lack a good emergency response plan. This can ultimately lead to a variety of negative consequences ranging from adverse publicity to significant operating losses as well as loss of life. On the other hand, those organizations that have come to realize that emergency response planning is vital have created and circulated elaborate policies and procedures designed to deal with a variety of emergency and disaster situations. Moreover, these organizations usually feel confident that they are prepared to deal with any contingency. Their emergency response plans detail specific actions to take in the event of a catastrophic event and outline specific steps that should be employed during the ensuing recovery effort. However, far too often, this is where the planning process ends. Typically, the planning document is filed away and forgotten until a critical incident occurs (Joyce and Hurth, 1997; Reid, 1996).

Emergency Planning Considerations

Clearly, no emergency response plan can be applied to every potential crisis situation. However, a comprehensive plan that takes into account potential natural, technological, and man-made threats and involves key personnel in the planning process can help an organization to systematically manage emergencies in an effective and efficient manner. Therefore, the planning process is a key element that forces security managers and supervisors to explore viable options that can be employed in the event of a critical incident. For this reason, oftentimes there is considerable discussion regarding which is more important, the plan or the planning process.

The Components of an Effective Emergency Response Plan

Being prepared for critical incidents involves four important components: planning, reviewing, training, and testing. These are the cornerstones of any emergency response plan and it should be noted that it is a circular rather than linear process. Perhaps Nudell and Antokol (1988) explain this concept best when they describe the above components, when implemented, as an umbrella of preparation against the thunderstorms of a potential crisis.

According to the American Society for Industrial Security's *Emergency Planning Handbook* (1994, p. 4), effective emergency planning begins with the following:

- Defining an emergency in terms relevant to the organization doing the planning
- Establishing an organization with specific tasks to function immediately before, during, and after an emergency
- Establishing a method for utilizing resources and for obtaining additional resources during the emergency
- Providing a recognizable means of moving from normal operations into and out of the emergency mode of operation

Incident Command System

With regard to establishing an organization with specific tasks and a method for utilizing resources, it should be noted that there exists a recognized system with a predetermined chain of command as well as a proven structure for an organized response to a critical incident. Referred to as the Incident Command System (ICS), it uses common terminology that is descriptive and decisive, yet not difficult to understand, in order to control personnel, resources, and communications at the scene of a critical incident (Woodworth, 1998; Dezelan, 1996).

ICS was developed in the early 1970s after a series of major wildland fires in southern California resulted in a number of recurring problems among emergency responders. Some of these included nonstandard terminology, nonstandard and nonintegrated communications, unmanageable span of control, and lack of the capability to expand and contract as required by the situation.

Although originally a fire service control system, ICS has since been adopted by a wide variety of local, state, and national emergency management and law enforcement organizations due to its many documented successes. Today it serves as a model all-risk, all-agency emergency management system. ICS principles have been proven over time in government, business, and industry. In fact, ICS has been endorsed by the International Association of Chiefs of Police (IACP) and the American Public Works Association (APWA) (FEMA ICS Instructor Guide, 1995).

There is also a legal requirement for using ICS since there are federal laws that mandate its use by individuals responding to hazardous materials incidents. Specifically, OSHA rule 1910.120, which became effective from March 6, 1990, requires that all organizations that handle hazardous materials use ICS. Non-OSHA states are also required by the Environmental Protection Agency to use ICS when responding to hazardous materials incidents (FEMA ICS Instructor Guide, 1995).

In essence, ICS is a well-organized team approach for managing critical incidents. It uses common terminology, has a modular organization (which means that it can expand/shrink according to the needs of the situation), has a manageable span of control (the number of subordinates one supervisor can manage effectively; usually 3–7, the optimum is 5), and uses clear reporting and documentation procedures. In effect, emergency response personnel can view ICS as an incident management toolbox. Not every tool in the toolbox will be used for every situation but the tools are available should they become necessary. Additionally, it is important to note that ICS can be used for all types of incidents regardless of size. However, it is essential that all emergency responders understand their specific roles when using ICS (Woodworth, 1998; Arata, Jr., 1995; FEMA ICS Instructor Guide, 1995).

The ICS structure is built around five major management activities or functional areas (FEMA ICS Instructor Guide, 1995):

- Command: sets priorities and objectives and is responsible for overall command of the incident
- Operations: has responsibility for all tactical operations necessary to carry out the plan
- Planning: responsible for the collection, evaluation, and dissemination of information concerning incident development as well as the status of all available resources
- Logistics: responsible for providing the necessary support (facilities, services, and materials) to meet incident needs
- Finance: responsible for monitoring and documenting all costs. Provides the necessary financial support related to the incident

These five management activities or functional areas form the foundation of the ICS organizational structure. The activities can be managed by one individual in the event of a small incident. Or, a fully staffed ICS structure, addressing all five functional areas, may be needed to manage larger or more complex events. In both cases, it is important to note that the Incident Commander is the individual in charge at the scene of a critical incident until properly relieved. The Incident Commander is also responsible for assigning personnel to the other functional areas (Operations, Planning, Logistics, and Finance) as needed.

ICS organizational structure (Figure 5.1) and procedures enable emergency response personnel to work safely together to take control of a critical incident. It can also assist organizations to effectively and efficiently manage the aftermath of a critical incident.

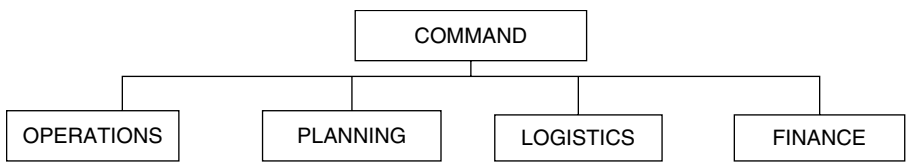


FIGURE 5.1 Basic Incident Command System organizational structure.

Common Requirements for Effective Critical Incident Management

Regardless of the type of crisis, Nudell and Antokol (1988, p. 4) point out that there are a series of common requirements that must be taken into account for an organization to be successful when a critical incident occurs. These include the following:

- Deciding policy
- Assessing threat
- Identifying resources
- Selecting crisis team personnel
- Locating the crisis management center
- Equipping the crisis center
- Training crisis team personnel
- Testing contingency plans and emergency procedures
- Dealing with the media
- Dealing with victims and their families
- Dealing with other affected persons (such as employees)
- Getting the organization's normal work done during the crisis
- Returning to normal after the crisis (both operationally and in human terms)

Vulnerability Analysis

With regard to the threat assessment above, many times this procedure can be accomplished by using a simple numerical rating system (scale of 1 to 5 with 1 as the lowest and 5 being highest) to list on a chart potential emergencies (such as fire, flood, and terrorist attack), estimate the probability of each emergency occurring, assess the potential human impact (death and injury), property impact (losses and damages), potential business impact (loss of market share), and finally, the strength of the internal and external resources that may be available (5 being weak resources and 1 indicating strong resources). Next, you would total the score for each emergency, taking into consideration that the lower the score, the better. Although somewhat subjective, the comparisons will be of significant assistance in determining planning priorities. The following example helps to illustrate the process (FEMA Emergency Management Guide for Business & Industry, 2006):

In the example shown in Figure 5.2, we would be most vulnerable to the fire scenario closely followed by the hurricane threat. We would be less vulnerable to the threat of an earthquake.

The Emergency Operations Center

An Emergency Operations Center (EOC) serves as a centralized area for the management of emergency operations. The EOC is where decisions are made by the emergency management team based on information provided by emergency responders and other personnel (FEMA Emergency Management Guide for Business and Industry, 2006).

Type of Emergency	Probability	+	Human Impact	+	Property Impact	+	Business Impact	+	Internal Resources	+	External Resources	=	Total
	L 1-5 H		L 1-5 H		L 1-5 H		L 1-5 H		W 5-1 S		W 5-1 S		
Fire	3		5		5		5		2		4		24
Earthquake	2		4		4		4		2		3		19
Hurricane	4		4		4		4		3		4		23

FIGURE 5.2 Vulnerability analysis chart.

The EOC can range from a dedicated, well-equipped center (comprehensive emergency communications capability including radio, telephone, fax, computer, and television; self-sustaining power sources; bathroom, eating, and sleeping facilities for staff; etc.) to an ad hoc room that is used as circumstances dictate. Of particular importance is that an organization identify its requirements ahead of time and establish the type of arrangement that best suits its needs (ASIS Emergency Planning Handbook, 1994; Nudell and Antokol, 1988).

Although the EOC should be near senior management, it should not interfere with everyday operations. In addition, an alternate site should always be selected ahead of time. Hawkes and Neal (1998, p. 54) state that "an effective command center ready to respond to any emergency is a critical component of any headquarters security plan." They further contend that "a successful command center is the result of careful planning, clearly defined structure and job descriptions and comprehensive training."

Media Relations

Procedures for dealing with the media is another important area that cannot be overlooked. When a critical incident occurs, the security manager will undoubtedly be pulled in many different directions. Faced with a considerable number of important tasks, the security manager may not view media relations as a primary concern. However, being prepared ahead of time to deal with the media can help an organization to get through the incident without the additional damage that can be caused by misinformation and speculation. In addition, the negative publicity that an organization receives as a result of a critical incident can have far-reaching effects. An organization's image and business can be adversely impacted. Litigation is bound to result as victims, the families of victims, employees, customers, and perhaps various interested outside parties will be seeking to lay blame and recover damages. Attorneys are bound to examine every newspaper account and TV report of the incident. They will, of course, be looking for statements from representatives of the organization for any admissions or confirmation that the organization was in some way negligent (Gardner, 1997).

Nuss (1997, p. 1) defines a crisis as "…an event requiring rapid decisions involving the media, that, if handled incorrectly, could damage the organization's credibility and reputation." He further provides a number of effective crisis communications steps that organizations should consider:

- Have a media plan
- Build a relationship with the media before a crisis strikes
- Train employees in crisis communications
- Maintain a good relationship with the media after [a] crisis

Cooperating with the media provides an organization with a number of important benefits that far outweigh the benefits of denying them access. In particular, it provides the organization with an opportunity to provide its side of the story. This is important since, oftentimes, the spokesman for the organization can make available background information that may provide a different perspective on the situation. Furthermore, working with the media may prevent reporters from seeking out secondary sources that are typically less informed and more likely to misrepresent the organization. Consequently, it is far better to have the organization give an accurate statement of the situation as opposed to leaving it up to the reporter to locate an "informed" source, which can lead to speculation and misinformation. Saying nothing also has its own risks. Ignoring bad news will not make the incident go away and usually this tactic raises additional questions (Gardner, 1997).

FEMA (Emergency Management Guide for Business and Industry, 2006) provides a number of important considerations for dealing with the media in an emergency:

- Designate a trained spokesperson and an alternate spokesperson
- Set up a media briefing area
- Establish security procedures
- Establish procedures for ensuring that information is complete, accurate, and approved for public release

- Determine an appropriate and useful way of communicating technical information
- Prepare background information about the facility

FEMA (Emergency Management Guide for Business and Industry, 2006) also provides the following guidelines when providing information to the media during an emergency:

Do's

- Give all media equal access to the information
- When appropriate, conduct press briefings and interviews. Give local and national media equal time
- Try to observe media deadlines
- Escort media representatives to ensure safety
- Keep records of information released
- Provide press releases when possible

Don'ts

- Do not speculate about the incident
- Do not permit unauthorized personnel to release information
- Do not cover up facts or mislead the media
- Do not put blame on the incident

It is quite evident that although safety issues are always a top consideration, a security manager or supervisor cannot overlook the importance of an effective crisis media relations plan. This plan must be implemented quickly during a critical incident in order to provide accurate and timely information while safeguarding the reputation and interests of the organization.

Developing the Emergency Response Plan

Obviously, the development of a comprehensive emergency management plan requires considerable time and effort and sufficient time should be provided for its completion. Representatives from key organizational units must be involved from its inception and upper management support is essential throughout the entire process. Many times this can be readily accomplished by having the chief executive officer or facility manager issue a mission statement that introduces the emergency management plan, its purpose and importance to the organization, and defines the structure and authority of the planning team. Additionally, it is important in the initial planning stages to select an individual within the organization to assume responsibility for the plan and act as the planning team leader or coordinator.

Ultimately, capabilities and hazards will be analyzed, specific roles and responsibilities will be carefully outlined, and critical company products and services will be identified in order to ensure a coordinated and effective response when a critical incident does occur. This will typically involve meeting with outside groups and establishing mutual aid agreements where appropriate. Gillespie (Drabek & Hoetmer, 1991) emphasizes that mutual aid agreements enhance preparedness and that emergency response is more effective when public and private organizations cooperate.

Some outside groups or agencies could include the following (FEMA Emergency management Guide for Business and Industry, 2006):

- Local police department
- Local fire department
- Emergency medical services
- City or county office of emergency management
- Local emergency planning committee (LEPC)
- City or county government officials
- Public works department
- Electric utilities
- Telephone companies
- Volunteer agencies such as the American Red Cross, the Salvation Army, etc.
- Essential contractors

- Suppliers of emergency equipment
- Company insurance carriers
- Neighboring businesses
- Trade associations
- National Weather Service

In crisis situations, organizations respond differently based on variations in tasks, level of preparedness, as well as political considerations. Conferring with outside groups or agencies ahead of time will undoubtedly avoid confusion and delays during the response phase of an emergency, improve coordination and communication during the management phase of the incident, and help organizations transition to the recovery phase much faster. However, it is important to note that these agreements should clearly define the type of assistance as well as the procedures for activating the agreement in order to avoid unnecessary conflict.

Reviewing and Integrating the Emergency Response Plan

Once the initial plan is completed, it is essential that its various components be reviewed in depth by planning team personnel and revised as necessary. The draft plan could then be presented to key management personnel as well as any individual who may be required to perform or provide support services. Many times, a tabletop exercise provides an excellent opportunity to review potential critical incidents with key personnel since problem areas can be readily identified and discussed. The plan can then be modified accordingly and later presented to the chief executive officer for final approval. On approval, the plan can be distributed to all affected personnel who should be required to sign that they have received the document. It is then important that the plan be quickly and clearly communicated to all affected personnel (Gigliotti and Jason, 1991).

It is imperative at this point that the plan be fully integrated into the organization's standard operating procedures (SOPs). According to FEMA (Guide for All-Hazard Emergency Operations Planning, 1996, p. 3–3), "SOPs and checklists provide the detailed instructions that an organization or individual needs to fulfill responsibilities and perform tasks, assigned in the EOP [emergency operations plan]…." Clearly, a comprehensive checklist that includes major planning, implementation, training/testing, response, and recovery components would be an invaluable asset to any organization's emergency response plan.

Training and Testing

After the plan has been finalized, communicated to all affected personnel, and integrated into the organization's standard operating procedures, it must be thoroughly tested. An emergency response plan will not work properly unless realistic training is provided and it is thoroughly tested prior to implementation in an actual emergency. Testing the plan helps to identify problem areas, as well as inherent weaknesses, that must be corrected in order to ensure that the plan will work as designed. Training and testing, thus, serve to identify areas in need of improvement, thereby enhancing coordination and communication among emergency response personnel.

The first step in the training process is to assign a staff member responsibility for developing an overall training plan and the requisite goals and objectives for each component. Additionally, a determination must be made as to the following:

- Who will actually perform the training?
- Who will be trained?
- What type of training activities will be employed?
- What materials and equipment will be needed?
- When will the training take place?
- Where will the training take place?
- How long will the training last?
- How will the training be evaluated and by whom?
- How will the training activities be documented?

- How will special circumstances be handled?
- How will training costs and expenses be budgeted?

It should be noted that critiques, or evaluations, are an important component of the training process and must be conducted after each training activity. Sufficient time should be allotted for the critique and any resulting recommendations should be forwarded to the emergency planning team for further review and action. Additionally, organizations should consider how to involve outside groups and agencies in the training and evaluation process. As previously mentioned, this could certainly help to avoid conflict and increase coordination and communication when a critical incident does occur. Emergency response training can take a variety of forms. FEMA (Emergency Management Guide for Business and Industry, 2006) describes six types of training activities that can be considered:

- Orientation and education sessions: Sessions designed to provide information, answer questions, and identify needs and concerns.
- Tabletop exercise: This is a cost-efficient and cost-effective way to have members of the emergency planning team, as well as key management personnel, meet in a conference room setting to discuss roles and responsibilities and identify areas of concern.
- Walk-through drill: The emergency planning team and response teams actually perform their emergency response functions.
- Functional drills: Designed to test specific functions such as medical response, emergency notifications, and communications procedures, although not necessarily at the same time. The drill is then evaluated by the various participants and problem areas are identified.
- Evacuation drill: Participants walk the evacuation route to a predesignated area where procedures for accounting for all personnel are tested. Participants are asked to make note of potential hazards along the way and the emergency response plan is modified accordingly.
- Full-scale exercise: An emergency is simulated as close to real as possible. Involves management, emergency response personnel, employees, as well as outside groups and agencies that would also be involved in the response.

Practical "hands-on" training always provides personnel with excellent opportunities to use skills that are taught and to learn new techniques and procedures. For emergency response training, simulations such as tabletop exercises, drills, and full-scale exercises are particularly valuable for practicing decision-making skills, tactical techniques, and communications. Moreover, simulations serve to determine deficiencies in planning and procedures that can lead to modifications to the emergency response plan (ASIS Emergency Planning Handbook, 1994; FEMA Emergency Management Guide for Business and Industry, 2006; Nudell and Antokol, 1988).

"Model City" Simulator

Perhaps one of the most successful and creative ways of teaching critical incident management to emergency response personnel is through the use of a "model city" simulator board. As the name implies, a "model city" simulator represents a small community with a residential area, business district, and industrial park. The simulator provides the realistic environment needed to give participants the feeling of actually having managed a critical incident and to immediately see the results of their actions. In essence, students get to practice decision-making skills in a realistic environment where there are no repercussions for making a mistake (BowMac Educational Services, Inc., 1992).

The goal of this training is to provide participants with a "game plan" that can make the difference in taking control of an incident or allowing it to mushroom out of control. The primary focus is on training operational personnel to manage the initial thirty minutes of a critical incident by employing a series of critical tasks or decisions. These include the following:

- Establish communications: Advise dispatch to hold the air and allow only emergency radio traffic or request that a separate frequency be assigned for the incident.

- Identify the "Hot Zone": It is very important to identify the "hot zone" immediately in order to limit additional exposure to danger.
- Establish an inner perimeter: An inner perimeter should be set up quickly. It is used to control and contain the area and prevent the initial situation from getting worse.
- Establish an outer perimeter: The outer perimeter is used to control access to the affected area. It is not an offensive position and should be located well outside of the "hot zone."
- Establish a command post: The command post should be established outside of the "hot zone" between the inner and outer perimeters. It does not need to be located with a view of the scene. Initially, the command post can be your vehicle or any other suitable temporary location with communications capability.
- Select a staging area: The staging area should be large enough to accommodate arriving emergency resources for transfer to the scene as needed. It must be located outside of the inner perimeter at a safe and secure location.
- Identify and request additional resources: Quickly assess the need for additional resources at the scene and direct resources to the staging area. Examples of additional resources are local police, fire, EMS, HazMat, public works, utility companies, the national guard, federal and state agencies, the American Red Cross, etc. (BowMac Educational Services, Inc., 1992).

The advantage of a critical incident management program using a "model city" simulator is that training shifts from discussing emergency response issues at the "tabletop" level to actually practicing handling an incident in a realistic, simulated environment. Learning to implement a standard set of tasks or procedures under these conditions will undoubtedly assist emergency response personnel to quickly take control and limit the growth of a critical incident, thereby affording a much greater opportunity for bringing the situation to a successful outcome (BowMac Educational Services, Inc., 1992).

Evaluating the Emergency Response Plan

Regardless of the training schedule selected, a formal audit of the entire emergency response plan should be conducted at least once a year. Furthermore, in addition to the yearly audit, the emergency response plan should be evaluated, and modified if necessary, as follows (FEMA Guide for Business and Industry, 2006):

- After each drill or exercise
- After each critical incident
- When there has been a change in personnel or responsibilities
- When the layout or design of a facility changes
- When there is a change in policies or procedures

Of course, any modifications or changes to an emergency response plan should be communicated to affected personnel as soon as possible. Similarly, changes to the planning document should be incorporated and distributed in a timely manner.

Terrorism's Impact on Crisis Management

The events of September 11, 2001, had a profound impact on the way the nation perceived the threat posed by terrorist groups. Despite a series of highly publicized and well-coordinated attacks on United States' interests abroad during the 1990s, the public was largely unprepared for the potentially catastrophic violence posed by small groups of committed individuals.

As security professionals it is easy to deride this lack of preparedness; however, it must be remembered that prior to September 11, 2001, the public's exposure to terrorism, while significantly troubling, did not come close to approaching the impact of the World Trade Center, Pentagon, and United Flight 93 attacks.

In the 1980s, terrorists' tactics generally included the hijacking of airliners and seizing of hostages to create uncertainty, promote fear, and engineer an environment of international

drama on which to publicize their cause. By the 1990s, terrorist tactics changed. While kidnappings still occurred, bombings and other high casualty-producing attacks became more commonplace. The attacks on the US Embassies in Tanzania and Kenya, as well as the bombing of Khobar Towers in Saudi Arabia, the seaborne assault on the U.S.S. Cole in Yemen, the domestic acts of terrorism on the Alfred P. Murrah building in Oklahoma City, and the first World Trade Center bombing in 1993 are but a few examples.

Over time, terrorist attacks have shifted from the deadly, yet limited, actions choreographed to obtain worldwide attention to catastrophic, casualty-dense attacks designed to shock the populace with high body counts while simultaneously destroying or damaging critical infrastructure (Stern 1999, Jenkins 2006, MIPT Terrorism Knowledge base http://www.tkb.org/, 9/11 Commission Report).

Post-9/11 Era: The Public Sector

In the days following the attacks on New York City and Washington D.C., the U S government, in direct response to the terrorist actions of 9/11, enacted significant changes to its security programs.

- President Bush issued an Executive Order to establish the Office of Homeland Security as part of the White House Staff.
- In March of 2002, the President issued Homeland Security Presidential Directive 3, authorizing the establishment of the color-coded Homeland Security Advisory System designed to alert government agencies, the private sector, and the citizenry to the changing risks of terrorist attacks.
- On November 25, 2002, President Bush signed the Homeland Security Act of 2002, which reorganized the reporting structure of 22 government agencies under the auspices of the newly created Department of Homeland Security (Haddow & Bullock 2006).

The purpose of these initiatives was to

1. Streamline the efforts of government agencies involved in security-related activities so as to increase cooperation and enhance efficiency
2. Reach out to the private sector in order to promote cooperation

The challenges in implementation, however, were enormous. Each agency had its own culture, management style, procedures, priorities, and sometimes, even rivalries. Only time and experience will tell how effective these efforts to reorganize the government's protective services have been.

Post-9/11 Era: The Private Sector

As is typical with high profile events, the initial reaction to the September 11 attacks was a flurry of activity to examine organizational security and business continuity issues. Budgets temporarily increased, as did the overall interest in security products and services. As time passed and attacks on the homeland were prevented in the short term, a separation process began to take hold. As one may expect, companies that deemed their risks to be lower reduced their budgets to pre-9/11 levels and went back to business as usual. Firms deemed to be at higher risk, such as utility companies, financial institutions, public venues, and organizations designated as critical infrastructure by the Department of Homeland Security, changed their security programs more significantly. Not surprisingly, the level of commitment to security, business continuity, crisis management, and disaster recovery expressed by the private sector is a result of perceived risk, vulnerability, potential impacts to operations, and a changing regulatory environment.

In the likely event that the war on terrorism becomes a long-term feature of US foreign and domestic policy, security, crisis management, business continuity, disaster recovery, and related disciplines will undergo the following changes:

1. More convention al terrorist attacks will be attempted in the United States.
2. Weapons of mass destruction will eventually be used against the United States.

3. Out of necessity, increased cooperation will occur between the public and private sector.
4. As critical infrastructure becomes more protected, soft targets such as shopping malls, schools, and movie theaters will become terrorist targets.
5. The demands for high quality security personnel will increase.
6. Government regulation regarding the selection and training of security personnel will increase.
7. Government regulation of recovery-related activities in the private sector will increase.
8. Demand for people with professional certifications, training and formal education in security management, business continuity, crisis management, and disaster recovery will increase.
9. The need for general education of the populace on terrorism and related issues will significantly increase.
10. Community Emergency Response Teams (CERT) will become a more prominent part of public safety.

Professional Development

An emergency response plan is a dynamic process that must be kept up-to-date and consistent with an organization's operations and identified vulnerabilities. Therefore, security managers and supervisors must continually scan their internal and external environments in order to anticipate and plan for problems that could have an adverse impact on their organizations. One way of accomplishing this is for security managers and supervisors to read extensively, become familiar with the numerous emergency/disaster organizations and services available, and maintain an active network with other professionals in their field, as well as in allied disciplines. Two excellent emergency/disaster-related resources to consider are the annual *Disaster Resource Guide* (Rainey, 2006) as well as the many resources available from various federal, state, and local emergency management agencies.

It should be noted that FEMA, through the Emergency Management Institute (EMI), offers an Independent Study Program consisting of a series of self-paced courses. Each set of course materials includes practice exercises as well as a final exam. The average time of completion is 2–14 hours and individuals who score 75% or better are issued a certificate of completion by EMI. The courses are offered free of charge to those who qualify for enrolment. In addition, college credit may be obtained after successful completion of the courses (FEMA Emergency Management Institute, Independent Study Program, 2007, http://training.fema.gov/EMIWeb/IS/).

Summary

Both public and private sector organizations are becoming increasingly aware of the need to plan for the effective management of critical incidents. Security managers and supervisors are expected not only to prepare well-written plans for these events but also to have a plan in place that works and is understood by all. This requires that the plan be tested through training, thereby ensuring that responding personnel can immediately initiate emergency management operations. Besides helping to define the technical, interpersonal, and organizational dynamics of critical incident management, these activities assist emergency responders to become familiar with the roles and responsibilities of all personnel, including outside groups and agencies, at the scene of a critical incident.

Bibliography

American Society for Industrial Security, Standing Committee on Disaster Management (1994). *Emergency Planning Handbook*. Dubuque, IA: Kendall/Hunt Publishing Company.

M. Arata, Jr. (1995). Finding order amidst the chaos. *Security Management* 39(9): 48–53.

BowMac Educational Services, Inc. (1992). *Critical Incident Management Instructor Notebook*. Rochester, NY: Author.

CSO Magazine Online. CSO fundamentals: The ABC's of physical and IT convergence. Retrieved March 2, 2007 from http://www.csoonline.com/fundamentals/abc_convergence.html

L. Dezelan (1996). Incident management system. *Law and Order* 44(8), Wilmette, IL: Hendon Inc.

T. Drabek and G. Hoetmer, eds. (1991). *Emergency Management Principles and Practice for Local Government*. Washington, D.C.: International City Management Association.

Federal Emergency Management Agency (2007). Independent Study Program. Retrieved March 2, 2007 from http://training.fema.gov/EMIWeb/IS/

Federal Emergency Management Agency (2006). *Emergency Management Guide for Business and Industry*. Washington, D.C.: US Government Printing Office.

Federal Emergency Management Agency (1996). *Guide for All-Hazard Emergency Operations Planning*. Washington, DC: US Government Printing Office.

Federal Emergency Management Agency (1995). *Incident Command System Instructor Guide*. Washington, D.C.: US Government Printing Office.

R. Gardner (1997). Getting ahead of the headlines. *Security Management* 41(7): 115–19.

R. Gigliotti and R. Jason (1991). *Emergency Planning for Maximum Protection*. Boston, MA: Butterworth-Heinemann.

G. Haddow and J. Bullock (2006). *Introduction to Emergency Management,* 2nd edn. Burlington, MA: Butterworth-Heinemann.

K. Hawkes and J. Neal (1998). Command performance. *Security Management* 42(11): 77–83.

B. Jenkins (2006). The new age of terrorism. In *The McGraw-Hill Homeland Security Handbook*, ed. David G. Kamien, New York, NY: McGraw-Hill Companies, Inc.

E. Joyce and L. Hurth (1997). Booking your next disaster. *Security Management* 41(11): 47–50.

T. H. Kean *et al.* (2004). *The 911 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (Authorized Edition). W. W. Norton, New York, NY.

MIPT Terrorism Knowledge Base. Retrieved March 2, 2007 from http://www.tkb.org/

M. Nudell and N. Antokol (1988). *The Handbook for Effective Emergency Management*. Lexington, MA: Lexington Books.

R. Nuss (1997). *Effective Media Crisis Communication During a Critical Incident*. Winter Springs, FL: Nuss and Associates, Inc.

R. Paschall (1992). *Critical Incident Management*. Chicago, IL: The Office of International Criminal Justice.

K. Rainey, ed. (2006). *Disaster Resource Guide*. Santa Ana, CA: Emergency Lifeline Corporation.

K. Reid (1996). Testing Murphy's law. *Security Management* 40(11): 77–78, 80–83.

J. Stern (1999). *The Ultimate Terrorists*. Cambridge, MA: Harvard University Press.

R. Sylves and W. Waugh, Jr., eds. (1996). *Disaster Management in the U.S. and Canada*. Springfield, IL: Charles C. Thomas.

B. Woodworth (1998). The incident command system: A tool for business recovery. *Disaster Resource Guide*. Santa Ana, CA: Emergency Lifeline Corporation.

Quiz

1. Preparing for emergencies involves four important considerations: _____, _____, and _____.

2. A particularly important component of the initial planning process is _____ analysis.

3. _____ are an important component of the training process and must be conducted after each training activity.
4. Emergency response training can take a variety of forms. List three types of training that can be considered: _____, _____, and _____.
5. A formal audit of the emergency response plan should be conducted how often? _____
6. The Homeland Security Act of 2002 reorganized the reporting structure of 22 government agencies, creating Department of Homeland Security. ☐ T ☐ F
7. Homeland Security Presidential Directive 3 authorized the establishment of the color-coded Homeland Security Advisory System. ☐ T ☐ F
8. Utility companies and financial institutions are considered "critical infrastructure" by the Department of Homeland Security. ☐ T ☐ F
9. During the 1980s, terrorist's tactics included actions designed to create uncertainty, fear, and international drama on which to publicize their cause. ☐ T ☐ F
10. Terrorist attacks have shifted from actions choreographed to obtain world-wide attention to catastrophic attacks designed to shock the populace and destroy critical infrastructure. ☐ T ☐ F

This page intentionally left blank

6 Supervising During Emergencies

Brion K. O'Dell

Supervising a security force can be challenging even during the best of times, but the real test of a supervisor's skill comes when an emergency arises. If not controlled, circumstances can quickly overwhelm both staff and resources with sometimes disastrous results. Depending on the type and severity of the incident, the security supervisor may find it is necessary to cope with the loss of utilities (such as lights and electrical power), property, communications, and transportation. There may also exist further complication of the medical needs of any victims or the necessity to institute crowd control.

As in other aspects of security, the key to success lies within the supervisor's ability to identify the most probable incidents likely to occur and to formulate adequate response plans to deal with them. These plans must take into account both natural and man-made threats.

Preparing for Emergencies

Developing Emergency Response Plans

When first developing emergency response plans, the wise supervisor will consult with all outside agencies that would be involved during a crisis. These should include local police, fire/rescue department, hospitals as well as utility companies, service vendors, or any other organization whose assistance or expertise would be needed during an emergency. Their experience can prove to be a valuable resource in identifying potential threats and formulating suitable responses. Coordinating your response plans with them PRIOR to an emergency will go a long way in avoiding confusion during an actual incident. The supervisor will find that in most instances the heads of these organizations are more than willing to offer their experience and training in assisting with the creation of emergency responses.

During this developmental stage, be certain to include appropriate staff from within your own organization: maintenance, safety, personnel, communications, legal, accounting, management, and so on. They will afford additional sources of information needed to formulate an adequate response plan. Adequate emergency equipment (fire extinguishers, first aid kits, two-way radios, flashlights, and so on) must be obtained and kept on hand.

Training/Practice Drills

Once a suitable response plan has been approved, it is essential to create a formal training program for all employees to ensure they have a complete understanding of its importance and proper implementation. This training must be comprehensive but also easy to understand. (Bear in mind these plans will be carried out during an emergency … a time when fear and confusion can cause people to panic.) Whenever possible, your training sessions should include representatives from outside agencies such as the police and fire departments. As

previously mentioned, their experience and training can prove to be an invaluable resource to your program. Periodic practice drills that include all employees should be held to help ensure smooth implementation in the event of a real emergency. Oftentimes serious flaws in a response plan can be uncovered and corrected during a practice drill that could otherwise lead to tragedy if left undiscovered.

Copies of the appropriate response plans should be kept accessible to all staff members and posted wherever possible. Evacuation routes must be clearly marked and adequate emergency equipments (such as fire extinguishers and first aid kits) must be readily accessible.

During the Emergency

When an actual emergency arises the security supervisor may be confronted by a myriad of responsibilities and challenges. While it is impossible to list every potential threat, it is possible to identify several areas of response that are common in most situations. It is important to note that the following are NOT listed in order of priority.

Implementation of Response Plans

The security supervisor MUST possess a thorough understanding of:

- The appropriate response plans and the steps that must be taken for their proper implementation.
- What outside agencies to contact in case of fire, medical, or criminal occurrence and what level of action is to be taken pending their arrival? (Note: The level of action taken by security officers will vary according to jurisdiction, state and local law, employer regulations, and so on.)
- Which evacuation routes are to be used?
- Which management and/or support personnel within their organization are to be contacted?
- What equipment and/or personnel will be required to contain the incident pending arrival of outside assistance?
- Proper procedures for handling inquiries from the news media, families of victims, employees, and so on.

Communication

No matter what the nature of the emergency at hand, the security supervisor MUST be able to maintain reliable communication with the security officers under his or her command and all other outside personnel involved (police, fire, medical, employees, management, and so on). This communication may be electronic, such as two-way radio or telephone or simply verbal. No matter how it is transmitted, information MUST flow between all parties involved. The supervisor must be able to communicate instructions to other officers and receive reports of activities as they occur. Likewise, emergency personnel must be able to provide information/instructions back to the security supervisor. Any major breakdown in the lines of communication could have disastrous consequences.

In today's high-tech world, the most frequently used method of communication is the two-way radio. While it is true that under most conditions radio can be used effectively, there are certain circumstances when their use would be prohibited. One such incident would be the investigation of a bomb threat (the use of a two-way radio could detonate a bomb). Under conditions such as these, alternate means of communication would be required.

The security supervisor must be able to adapt to changing situations and have backup methods of communication at hand.

Coordination of Activities

During an emergency it is likely that several outside emergency agencies would be involved. This means a large number of personnel may all be working together. In order to prevent

confusion (with potentially deadly results) the activities of all involved must be coordinated into an organized effort.

If, for example, the supervisor was confronted with a fire, the activities of the officers under his or her command would need to be directed pending the arrival of the fire department. Once the fire department personnel were at the scene, their command officers would take charge. The security supervisor would need to inform them of the location and nature of the fire, the location and condition of any victims, the actions taken by the security staff, and so on. While it is the responsibility of the fire department to contain/control the incident, it is quite possible that the fire department would direct the security staff to assist them in their efforts with such duties as crowd control, aiding victims, locating witnesses, and so on. As it is highly unlikely that the security staff would have direct radio contact with the fire department personnel, the job of relaying information and instructions would most probably fall to the security supervisor.

While a fire is only one of the many potential incidents the supervisor may confront, the need for effective coordination of activities holds true in all emergency situations. The security supervisor must be able to cooperate with all other outside emergency personnel and to assist them in successfully bringing the emergency under control.

Protection of Assets

During the height of an emergency, the security supervisor may find the first priority is to assist any victims. While this indeed should be the top priority, the supervisor must not overlook the necessity of protecting the assets of his or her employer. These assets would include all property, equipment, merchandise, vehicles, office supplies, and so on.

The confusion and distractions that can arise as the result of a serious incident can afford others the opportunity to remove or damage property with little or no chance of detection. Additionally, the increase in the number of persons that may be present at the scene of an emergency can cause valuable evidence to be removed or inadvertently destroyed.

The security supervisor must be able to utilize all available officers and resources to contain/preserve the scene while implementing all necessary procedures in order to prevent unauthorized persons from entering the scene regardless of their intentions.

Depending on the type and severity of the emergency, the supervisor may suddenly be confronted with the loss of resources and equipment that normally are taken for granted. Alarm and intrusion systems may be inoperable. Access controls and barriers such as fences, doors, security screening, and so on may be damaged and no longer able to deter unauthorized entry. Valuable equipment or merchandise may become exposed and vulnerable to attack. It may be necessary to arrange for a temporary increase of security personnel from outside sources or to obtain additional backup equipment in order to effectively protect the area.

The security supervisor must be able to quickly adapt to changing situations, effectively utilize all available resources and manpower, and take whatever actions are necessary to preserve and secure the scene.

Conclusion

It is not possible to list all of the possible contingencies the security supervisor may encounter during his or her career. However, it is quite clear that in order to be effective, he or she must be adaptable, able to communicate, possess the ability to remain calm under pressure, be familiar with all applicable procedures, and to continually hone his or her skills through practice and continuing education.

Supervising During Emergencies

Quiz

1. In order to prepare for emergencies, the supervisor should identify the most probable _____ likely to occur and formulate adequate response _____ to deal with them.
2. When developing the response plans, the supervisor should consult with all outside _____ and with _____ within their own organization.
3. Once an appropriate response plan has been created, a formal _____ should be held, followed up with routine _____.
4. The supervisor should consult with outside agencies whenever possible because their _____ and _____ can be valuable _____.
5. During certain emergencies, the supervisor may be faced with the loss of _____ that are normally taken for granted.
6. During an emergency, the security staff must handle all situations themselves. ☐ T ☐ F
7. The only form of communication the security supervisor will need during an emergency is two-way radios. ☐ T ☐ F
8. Once outside emergency personnel have arrived the security supervisor will have no other responsibilities or duties ☐ T ☐ F
9. During an emergency the security supervisor's top priority is the protection of the employer's assets. ☐ T ☐ F
10. The security supervisor must be able to adapt to changing situations. ☐ T ☐ F

7 Supervising During Special Events

Christopher Innace

The role of a security supervisor is a challenging one, often requiring planning and communicating with various entities. Special events such as rock concerts, athletic events, speeches, autograph sessions, political rallies, or stockholder meetings pose a unique set of challenges. There are many potential risks at special events that security supervisors should be aware of, the major one being violent crowds. This cannot be stressed enough. Crowds are capable of extensive violence and destruction, oftentimes unleashing their fury in an explosive manner. Effective crowd management is a major step in avoiding a disaster during special events.

Additionally, special events provide an opportunity for image enhancement, both of the protection entity as well as the parent or client organization. In some cases, projecting a positive image and relating well to visitors, customers, and the public at large is the sole reason for the existence of the parent/client or security organization. Shopping centers, amusement parks, and stadiums all exist for the comfort and entertainment of patrons. Supervisory personnel who wish to thrive in their professional careers need to exploit this opportunity to the greatest extent possible!

Assessment

There are many options to consider when assessing for crowd management. The security supervisor must work with the facility and venue manager to have an effective plan. Together, they should try and ascertain the characteristics of the crowd/audience due at a particular event. Assessing the size and nature of a crowd is important for a security supervisor. The size of a crowd can be determined by ticket sales, counting seats, etc. The nature of the crowd may be determined by the event itself. For example, if it is a football game, then crowds tend to be rowdy. One can estimate that alcohol will be a factor in changing some persons' behavior in this type of crowd. If it is a gymnastics crowd, for example, then the crowd tends to be calmer and more relaxed.

There are five different types of crowds that a security supervisor should be aware of:

Acquisitive crowd—is one motivated by the desire to get something. They are concerned with their own interest in buying merchandise, getting an autograph, or shaking the hand of a celebrity. As long as their desires are met quickly and efficiently, they are easily managed.

Expressive crowd—usually is when crowd members express their feelings at a protest, demonstration, or convention. This type of crowd is usually well behaved but can easily become hostile if the proper causal factors are present.

Spectator crowd—usually gathers to watch an athletic event or some type of entertainment. A concern here is that emotions can change rapidly, especially during sporting events. Troublemakers must be spotted and dealt with early on and the crowd as a whole continually assessed as to their mood.

Hostile crowd—is motivated by feelings of hate and fear. This type of crowd is ready to fight for what they believe in. This usually occurs at strikes, riots, or political demonstrations. Obviously, plans must be made to immediately implement dispersal procedures.
Escape crowd—are crowds that try to flee. This can occur due to an emergency situation such as a fire or other sudden disaster event. Escape crowds can also be created due to mismanagement by protection forces. Care must be taken to ensure that crowds do not become too large or confined. There must also be the ability to see and hear by all crowd members, especially those at the extreme front and rear. Quick, efficient, orderly evacuation routes must also be established.

There are five psychological factors of crowd members that a security supervisor should make note of:

Security—Some people possibly will join a crowd because they feel that they will be safe since many others are there as well. For example, this can occur if a gang is threatening citizens and some of the citizens join the gang for security purposes.
Suggestion—By joining a crowd, people accept ideas of the leader and can forget about their own beliefs, values, morals, or basic common sense.
Novelty—A person may enter a group to get away from his normal routine or regular duties. He feels like he belongs to a new adventure. This is usually due to some influence from the crowd leader.
Loss of identity—One loses one's sense of individuality—and individual accountability—being in a crowd. One believes that one can act with impunity and so will engage in deviant behaviors that one would not normally entertain.
Release of emotions—In an emotionally charged crowd, one's faults (anger, hostility, etc.) can surface. This gives the crowd member a chance to do things that he normally would not do.

The International Association and Campus Law Enforcement Administrators (IACLEA) offers their members an e-mail service which can be very useful. A security supervisor could gather information via this service from other protection professionals. An example of this is:

Date: Th. 20 Dec. 20__ 15:30
From: "Christopher Innace" >cinnace@ycp.edu<
To: IACLEA-L@iaclea.org
Subject: Aerosmith
I am looking for any information on any problem related to the group Aerosmith performing at other campuses. They will be performing here 2/16/20__ and part of their contract is that they will have security assigned to them on campus.
Thank you.

Access Control

Barriers play an important role as to who gets allowed onto the premises. Who gets in and where they can go requires decision making by the security supervisor and venue management. Criteria for spectators in getting into the facility can be tickets and a guest list. Employees—and in some cases visitors—should have identification cards. These cards should have numbered or colored zones placed on them so the security officer and the employee know where they can and cannot go.

Other decisions depend on if the facility has gates or doors that lock up the outside premises. The security supervisor must decide with facility/venue management when to open and close the facility for employees, performers, athletes, etc. Other barriers that must be checked constantly are entrances and exits. First of all, how many are there and when do they need to be locked or unlocked?

Communications

Communication is an integral component of preparing for a special event. All communication equipment should be tested prior to the event. The security supervisor should establish a method for security, venue management, and law enforcement agencies to be able to contact each other. This can be accomplished via radios equipped with multiple channels. Backup battery packs and spare radios are also essential to the security supervisor. Other communication equipment to be used should include enough telephones, cellular phones, intercompany phones, and "bell line" phones to handle the increased traffic required during emergencies. A public address system in the facility can be very useful also as well as portable PAs ("bullhorns") and whistles.

In many facilities, large video monitors are placed at strategic locations to provide entertainment, information, or emergency instructions to crowd members or employees. These monitors can keep the attention of crowd members focused in a positive manner, especially if there are periods of waiting. Spectators are entertained and not as easily aggravated by having to wait in line. This can easily be tied into the parent or client organizations' marketing effort by providing information on sales, promotions, upcoming events, etc.

Protection officers should have all of their lines of communication checked for both transmission and reception capabilities at the beginning of each shift. There should also be periodic checks to ensure that radio batteries are at proper strength, "dead zones" are avoided, etc. Officers should always think in terms of backup communications in case the primary method of communication is not useable for any reason. This should be stressed and reinforced at every opportunity!

Traffic Control

Traffic control is essential during special events especially when there are emergencies. No emergency plan can succeed without effective traffic control systems in place. It is also important for public relations purposes as it is at this juncture that visitors first come into contact with representatives of the facility—the protection officers directing traffic.

Officers must possess the proper equipment when assigned to traffic control duty. A flashlight, radio, and whistle are necessary. Also, officers must dress according to the weather so that comfort is assured during long hours. For safety and public recognition purposes, officers should dress so as to be visible. Reflective body vests should be required so that both ease of recognition and officer safety are enhanced.

There should be a separate lane cleared out in case of a fire or other emergency situation. Being able to quickly remove injured persons, evicted individuals, and arrestees is important. Being able to bring in fire equipment, vendor supplies, or additional personnel efficiently is also a key to successful event management. It is also advantageous to be able to do this without crowd members seeing the ambulance, arrestee, additional personnel, etc. arriving or departing. Prudent security supervisors make sure these lanes of approach and exit are kept open!

Training of protection officers in proper traffic control procedures is essential to the security supervisor. Initial and periodic refresher classes must be given to ensure proficiency. Improper procedures, such as incorrect hand signals, could lead to accidents, so training to prevent these behaviors and continuous supervisory assessment on-the-job are essential. Checking the proficiency of officers and the appearance/image of traffic control points is an essential supervisory function. Finding deficiencies and correcting them before they blossom into serious problems is the key.

When officers direct traffic, signals should be simple and distinct. Appropriate sign placement is also essential to both manage traffic and project the proper image. Supervisors

should address the traffic control function from a system's perspective. Each part of the traffic control system should act in concert with the whole.

Emergency Medical Operations

The security officer should be trained in first aid. When dealing with a person who is sick or injured, first communicate with the patient if possible. Then, the officer should provide basic first aid if necessary. The next step is to call for assistance (911) and to then manage crowds and bystanders. The officer must stay with the patient until medically trained help arrives. Medical personnel (EMTs) to visitors should be a ratio of 1:750. Certified EMTs are essential for the purpose of emergency medical operations.

Provision must also be made for ambulance service. In some facilities, patient transport can be accomplished via golf carts or similar types of patrol vehicles. In-house ambulances may also be used. In all situations, external ambulance capabilities must be assessed. Similarly, emergency room capabilities at local hospitals must be factored in, should there be mass casualties.

Evacuation

In an indoor facility, a six-foot "clear zone" around the inside of the perimeter must be maintained for evacuation purposes. Any equipment must be secure and out of the way in case of a panic situation arising. The security supervisor does not want this to interfere when crowds head toward the exits. For an outside event, plans must be made and discussed concerning evacuation routes.

In addition to routes, there must be areas that evacuating crowd members can congregate in. These areas must be large enough to accommodate everyone and provide for the safety of everyone. There should also be consideration given to what crowd members do after evacuating, such as getting in their cars and leaving or assembling and being advised on where to go next.

Fixed Posts

Fixed posts manned by security personnel are a necessity for any special event. At every fixed post, post orders are a must. Post orders must be clear and understandable so a person unfamiliar with security concepts can comprehend the orders. Every security officer manning the post should know the objective or mission of the post. The location of the post should be included in the post order. Manning orders should also be included to stipulate when the post is operational, as well as what type (unarmed, armed, male, female, etc.) and how many personnel man it.

Any equipment used should be listed and tested regularly. When first manning the post, there should be a sign-in sheet logging the use of any equipment for the security officer to sign. Some equipment common to fixed posts are portable radios, flashlights, rain gear, batons, fire extinguishers, and CCTV monitors. There are also many other types of possible equipment that may be used, contingent upon the operational and emergency needs of that post. Also, duties must be specified in a post order. This includes area of responsibility and an establishment of a route of retreat, should hostile crowd actions necessitate this.

Sample Post Order

Objective:	To check and collect tickets.
Location:	Aquatic Center—Gate A—Stand right beside turnstile.
Manning:	Hours of post are from 1300 to 1600 hours by a singleunarmed officer.
Equipment:	Sign sheet for portable radios and flashlights. Make sure theyboth work. Perform a radio check with the command post or CAS every hour.

Duties:	Check tickets for date, time, and the event to make sure that the tickets arenot counterfeit. Rip tickets in half and place one half in the box besideyou and return the other half of the ticket to the ticket holder.
Emergency route:	Exit Gate A and proceed north to parking lot 14. A supervisor will meet you there.

Assigning Security Officer's Posts

There are a myriad of different assignments at posts. An example of a post order can be checking identifications at an assigned area. Another possible post order can be checking tickets or baggage at the spectator entrance. Another could be observing crowd behavior at a special event, strike, or the scene of a recent fire.

Examples of posts for a sporting event include:

Main door	Locker rooms entrance/exit
Hallways	Spectator entrance/exit
VIP entrance/exit	Seating areas
Media entrance/exit	Parking lots
Athlete entrance/exit	Delivery entrance/exit

Pre-event Briefings

The security supervisors should have briefings before the security officers go to their posts. These meetings should be brief and explain/remind everyone of what is expected. They should be planned and structured, using a predesigned outline of what is to be covered. The supervisors should go over different responsibilities, objectives, and approaches. They should make sure that everyone has their proper uniforms on and is ready to meet the public! A review and check of equipment should be performed. The supervisors should make sure that officers know how to use everything and that each piece of equipment is functional. This is especially important with weapons and communications equipment.

Most important, ascertain that security officers know exactly what is expected of them! Clearing up any questions they may have is an absolute necessity.

Talking to Crowds

Communicating with crowds properly may prevent problems from occurring. Unfortunately, in many instances, proper preparation has not been made to accomplish this. When addressing a crowd, there are some steps that a security supervisor—as well as his/her subordinates—should follow:

1. Think before saying something so that the message is clear and concise.
2. When trying to relay a message, first get the crowd's attention through sound (whistle or clap) or verbal message ("May I have your attention?").
3. Speak slowly and clearly.
4. Project voice to the farthest person but do not try to yell.
5. Use eye contact to express authority. Be somewhat direct with eye contact.
6. Try to make eye contact with every person in the group.
7. Be calm and relaxed.
8. When directing a crowd to move on, do not make exceptions allowing anyone to remain.
9. Be firm. Be assertive.
10. Be polite.

Post-event Briefing

Debriefing should always take place after the event. Here the security supervisor goes over how everything took place. There should be an overall summary between the security supervisor and venue management. Comments and recommendations should be discussed.

Some tips can include discussions on any possible problems with the security personnel. It also should contain comments on the overall security of the special event. This includes exterior and interior security.

Sample Post-event Assessment Form

Event: _____
Date: (From—To) _____
Attendance: _____
# of supervisors: _____
# of security: _____
Promoter: _____
# of accidents/injuries: _____
# of incidents: _____
Brief summary of any incidents, accidents, or injuries: _____
Comments: _____
Recommendations: _____

The crowd management process can be conceptualized as a system with various components. These components include:

1. Selection
2. Application/interviewing
3. Testing
4. Training

Selection

The type of individual hired is a key managerial aspect in any job. It determines the level of performance expected. It is especially important for crowd management. As a security manager, the type of individual hired is one who is smart, calm but decisive, assertive with an ability to communicate precisely and professionally.

Other personal skills should include:

1. team player
2. service attitude
3. mature personality

Many times, security managers hire their personnel *en masse* for special events without doing any testing or without in-depth interviews. There should be minimum standards established.

Sample Security Officer Requirements

High School Diploma
Previous training in public relations

State certified security officer license—if applicable
Minimum of 5 years of security experience preferred
Excellent physical condition
Possible college degrees—criminal justice, asset protection, public relations majors
No convictions other than minor traffic violations

Recruitment

Recruitment is essential to acquire efficient security officers. Recruitment establishes the parameters of the selection pool. Recruitment can be accomplished by a variety of approaches. A few that might be applicable to special event staffing are:

Visiting different schools: Recruit students majoring in criminal justice, security programs. Also, recruit students with customer service skills and previous security jobs.
Advertising in paper/use of media: Good method because it will get many applicants but many times it attracts people who want to work a short time before becoming a police officer.
E-mailing: E-mail security/campus directors at different colleges and universities. This can be an effective way to acquire qualified applicants. This may work well with agencies that only require periodic staffing.

Applications/Interviewing

Applications must be studied carefully, since job seekers tend to exaggerate. Some things to look for during the screening process include:

1. Indications of being clearly overqualified
2. Unexplained gaps in employment history
3. Gaps in residences
4. Indications of lack of job stability
5. Inadequate references

When interviewing a prospective employee, yes or no questions should not be asked—at least not during the initial phases of the interview. These questions do not require the interviewee to think on the spot and explain themselves clearly and concisely. These latter skills are what is assessed during an interview. They are essential attributes for crowd management personnel to possess. While interviewing, answers to questions should be compared to the application and resume. The job candidate's verbal responses, the resume, and the application form should all be audited against each other.

Testing

After the interview stage, certain specific tests are recommended. These tests may include:

Psychological assessment such as the Minnesota Multiphasic Personality Inventory (MMPI)—these assessments can reveal habits, fears, sexual attitude, and symptoms of mental problems. They may also help to classify a person's personality.

Honesty tests—these help employers screen job candidates because they measure trustworthiness and attitude toward honesty.

Drug tests—can help because employers expect their workers to perform their duties free of intoxicating substances. Also, some security service firms advertise on the basis of their drug screening efforts.

Background investigations should also be required, including a federal background check. An applicant's criminal history is an area of concern to employers especially when an applicant is applying for security employment. Failure to effectively screen personnel who are in positions of trust and who subsequently violate that trust can result in extensive civil litigation.

Training: A Supervisor's Responsibility to the Employee

When dealing with crowds, it is important that security personnel be trained effectively to handle various situations. There are many approaches that can be taken to training. Essentially what must be done is to ensure that all necessary competency areas are covered thoroughly. A job task analysis should be performed before initiating training to insure that this occurs. Once this is done, a list of topics or competency areas can be constructed.

Sample training topics

Crowd control
Report writing
Safety
Patrol techniques
Traffic control
Bomb threats
First aid
Fire prevention/control
Emergency planning
Alarm systems

Hazardous materials

VIP protection
Hostage situations
Public relations

Delivering Instruction

1. Be patient, keep the learner interested, find out learner's background, and prepare for instruction.
2. Determine what must be taught and decide how much to teach.
3. Maintain records of training in order to know how much has been taught and which person has been taught what by whom.

Orienting New Officers

This phase of training tells each new employee what is expected of them and also what the employee expects (feedback). Orientation also provides an overview of job requirements and tasks.

On-the-Job Training Phase

1. Explain and demonstrate each job step.
2. Make sure employee comprehends!
3. Document training by having forms with all areas that have been covered and taught and have this signed by the employee.

Equipment

Another integral aspect of a security officer's training is his/her knowledge of equipment. There is a wide variety of equipment that the security officer must be able to handle at any given moment. Magnetometers, hand-held wands, flashlights, radios, and first-aid equipment are all indispensable to any security job. Metal detectors can be very important in helping to ensure that weapons do not enter the premises. Specific, documented instruction should be given on each piece of equipment used during both routine and emergency conditions.

Conclusion

Preparing for a special event is a considerable undertaking. Persons with supervisory responsibility who are involved in asset protection must approach this task in a serious manner. The supervisor should be detailed, thorough, and flexible in his/her approach. Continuous professional growth is strongly recommended. Constant checking of personnel performance is required. Nothing can be left to chance when providing protection at a special event.

Bibliography

P. C. Bishop (1998). Crowd control management and procedures. In *Protection Officer Training Manual*, eds. S. J. Davies and R. R. Minion. Boston: Butterworth-Heinemann.

S. J. Davies and R. R. Minion, eds. (1998). *Protection Officer Training Manual*. Boston: Butterworth-Heinemann.

D. S. Estes (1995). Supervision and training. In *Security Supervisor Training Manual*, eds. S. J. Davies and R. R. Minion. Boston: Butterworth-Heinemann.

C. A. Hertig (1995). Supervisor's role in training. In *Security Supervisor Training Manual*, eds. S. J. Davies and R. R. Minion, Boston: Butterworth-Heinemann.

C. A. Hertig (1985, June). Keep your guards posted. *Security Management*, 65–66.

A. A. Holm (1998). Traffic control procedures. In *Protection Officer Training Manual*, eds. S. J. Davies and R. R. Minion. Boston: Butterworth-Heinemann.

M. J. Millsaps (1998, Spring). The F.A.S.T. approach. *Protection News*.

K. C. Poulin (1992). *Special Events: Avoiding the Disaster*. Florida: International Foundation for Protection Officers.

P. Purpura (1991). *Security and Loss Prevention*. Boston: Butterworth-Heinemann.

K. Tyo (1996, Jan–March). Olympic security: A crowd management interview. *Crowd Management*, 6–11.

C. W. Sherwood (1998, August). Security management for a major event. *Security Management*, 9–16.

Task Force on Crowd Control and Safety (Sept. 29, 1998). Crowd management: Report on the Task Force on Crowd Control and Safety. http:www.crowdsafe.com.

For More Information

Special Events Planning by K.C. Poulin is published by the International Foundation for Protection Officers. Call (239) 430-0534 or visit www.ifpo.com.

The Protection Officer Training Manual is the official text for the Certified Protection Officer (CPO) program. The Manual contains chapters on Crowd Management, Public Relations, Emergency Situations, Traffic Control, etc. It is available for purchase from Butterworth-Heinemann. Call (800) 366-2665 or visit www.bh.com.

The Professional Security Television Network has various videos related to Crowd Management, as well as many other titles. Call (800) 942-7786 or visit www.pstn.pwpl.com.

Advanced Systems Technology, Inc. High Impact Training Solutions; 4111 W. Gore Blvd., Lawton, OK. 73505- 888-903-5387 -www.hits.astcorp.com

York College of Pennsylvania through the Office of Community and Professional Development offers seminars in Crowd Management, Public Relations, and other related topics. Call (717) 815-1451 or special programs@ycp.edu or visit www.ycp.edu/.

Supervising During Special Events

Quiz

1. In some cases projecting a positive image and relating well to visitors, customers, and the public at large is the sole reason for the existence of a security organization.

2. List the five different types of crowds:
   a) _____
   b) _____
   c) _____
   d) _____
   e) _____

3. List the five psychological factors of crowd formation:
   a) _____
   b) _____
   c) _____
   d) _____
   e) _____

4. In regards to communication at an event the security supervisor should establish a method for _____, _____, and _____ to be able to contact each other.

5. Protection officers should have all their lines of communications checked for both _____ _____ and _____ capabilities at the beginning of each shift.

6. What element is most essential during events, especially when there is an emergency?
   a) Positive image
   b) Access control
   c) Traffic control
   d) Force

7. Checking the proficiency of officers and the appearance/image of traffic control points is an essential supervisory function. ☐ T ☐ F

8. ` Medical personnel (EMTs) to visitors should be a ratio of:
   a) 1:500
   b) 1:750
   c) 1:1,000
   d) 1:2,500
   e) None of the above

9. In an indoor facility what is the necessary "clear zone" around the perimeter that should be maintained for evacuation purposes?
   a) Three foot
   b) Twenty foot
   c) Hundred foot
   d) Six foot

10. The type of individual hired is a key managerial aspect in a security supervisor's job as it determines the level of performance expected. ☐ T ☐ F

8 Security and Medical Response

David W. Hill

As the subject matter of this chapter is too broad to be taught in depth over the next few pages, this section will demonstrate the relationship between security and emergency response. Rather than providing detailed, "how-to" information, the discussion will focus on the importance of developing a range of skills. It is the responsibility of every security professional to become skilled in security and emergency response through continuing education.

What is Emergency Response?

First aid may be defined as the temporary care of the sick or injured. This care extends from the moment you assume responsibility to a time when the patient can be transferred to the care of a medical facility. Temporary care could include the saving of a life and preventing injuries from worsening. The three principles of first aid are:

1. Preserve life
2. Prevent an injury or illness from becoming worse
3. Promote recovery

The growth of emergency medicine as a specialty in the last decade has enhanced the quality of care given to the injured. The competence of all emergency medicine providers has come under close examination.

The Emergency Medical System (E.M.S.), developed and controlled by local provincial and state governments, is the medical system by which patients are transferred to the nearest or required medical assistance. During a basic E.M.S. response, the local hospital or ambulance dispatch center receives the emergency call. All pertinent information is quickly recorded through local protocol and an immediate decision is made as to the nature and priority of the call. If an ambulance is required, it is dispatched immediately and the personnel are advised of the situation. The ambulance crew is in constant communication with the dispatch center and relay patient information as they progress through their response. Call information can be relayed from dispatch to the hospital or a radio patch can be initiated enabling the ambulance crew to speak directly to the hospital staff. The patient is then transferred to the hospital which has been notified in advance, as quickly as the nature of the call dictates. Upon arrival at the hospital, the patient's vitals and history are submitted.

Economics of Security and Emergency Response

Over the last 10 years, we have witnessed an historical revolution in progress. The world population is at an all time high, while unemployment is at an all time low. Famine and crime are rampant and many nations are at war due to intolerance and economic hardship. New diseases such as AIDS are challenging mankind, while forgotten diseases are making

a comeback and have arrived in North America. Tuberculosis, to name one, is very contagious and often fatal if left untreated. The security/emergency medical responder would be well advised in today's society to become familiar with all aspects of disease prevention. An ounce of prevention is worth a pound of cure, especially since your life as a medical responder may depend on your knowledge and expertise.

When dealing with patient trauma involving blood, the security officer should wear medical gloves to prevent crosscontamination of diseases such as Hepatitis B, a liver disease. Due in part to such medical considerations, a new breed of security officer, professionals skilled in both security and emergency response, is being created.

Economic Factors

One of the main focuses of corporations today is streamlining the workforce—getting the maximum for the minimum. Effective cost reduction is essential to any corporation wishing to be successful in today's market. Many jobs are being lost due to automation and cutbacks. To ensure your position as a security officer, you must seriously consider crosstraining.

The old adage of giving someone their money's worth is now becoming a matter of survival in the workplace. An interesting note is that you will often find that many corporations are willing to pay fewer people higher wages in exchange for varied skills.

The various responsibilities of the modern-day security officer are expanding due to cost cutting and the personal safety issue. You must be aware that the workforce of any corporation is a community within itself. Each person has individual life experiences, difficulties, and a medical history. As a security officer, you may be called upon to respond to a variety of medical emergencies. How well you handle such situations may well be the difference between life and death.

Legal and Medical Obligations

Your responsibilities to your employer and workforce may be legal, medical, or both simultaneously. It is important to familiarize yourself with both your legal and medical obligations to ensure you are aware and in control of any given situation.

Consider the following scenario: an employee is observed trying to leave the job while appearing to conceal something. You politely ask the employee what it is and if you may see it. The employee states that he/she is doing nothing wrong and that it really isn't any of your business. You, as a company agent, persist in your questioning and an argument ensues. (Note: If this were a store customer you could be getting into legalities with which you should be familiar.) The security officer at this point could be dealing with laws such as assault, unlawful confinement, illegal search, and seizure or unlawful arrest if the situation proceeds that far. What if the suspects suddenly keel over clutching their chest? You must be prepared to switch from your role as a security officer to that of an emergency medical responder. The suspect, now referred to as a patient, is still angry at you and refuses your assistance. What would you do and how would you react to this situation? Cross-training could provide you with the appropriate skills to deal with such circumstances.

Everyone has Rights

If you were to sit down and study the *American Bill of Rights* and the *Canadian Charter of Rights and Freedoms*, you would quickly realize people, including security professionals, have a lot of rights. Through your studies you will become aware of state, provincial, and federal laws. Any infringement on a person's rights may lead to losing a case in court and could cause you, your department, and your employer great embarrassment. An interesting point is that laws protecting people's rights relating to crime are just as binding when dealing with a medical response. The right of privacy is a basic and fiercely guarded privilege in our society that cannot be violated even for the best of intentions.

We in the security profession are not peace officers, nor do security officers normally have peace officer status. However, the Canadian railway police (security) possess full police powers within a specified distance from railroad property and security officers employed by

the Public Service of Canada are designated public officers under the Financial Administration Act. In the United States, some states require that protection officers be "commissioned" or accredited as peace officers by the state. Protection officers in these states are granted full or limited police authority and are also subject to the same legal restrictions placed on this authority by the U.S. Constitution, state statutes, and local ordinances.

Even during a medical response, security officers usually have no more powers of arrest than those of an average citizen. While responding to an on-site medical call, you must attain some sort of consent. That is, the person's consent to be touched and aided. The following are guidelines for acquiring consent:

1. A person may not be coerced into medical treatment if they do not want it.
2. A person has the supreme legal right to be free from being touched against his/her will.
3. Treatment given to a person, even if in good faith, and performed with a degree of competence, may still be held to constitute assault unless proper consent has been obtained from the patient.
4. Consent may be given in writing, given orally or may be inferred by the actions of the patient. Something as simple as a hand being held out for help will suffice.
5. Consent must be voluntary.
6. The patient must be mentally and physically able to decide whether or not he or she wants treatment. Watch out for the gray area here. If the patient is deemed incapable of taking a rational decision regarding his own welfare, quickly contact a doctor and/or the police to take the patient into protective custody.
7. If the patient is unconscious, the consent is automatically implied. The law will regard the unconscious patient in immediate need and will assume that the patient would have consented to assistance.

The only occasion where an act can be performed on a patient without his/her consent is an emergency. An emergency allows for the necessary treatment to be undertaken or for the extension of the treatment. Since no consent has been given, the burden of proof rests with the caregiver. Thus, the following criteria are necessary and should be well documented to prove that an emergency existed:

1. A threat to the life or health of the patient must exist.
2. The threat must be immediate.
3. It must be impossible to obtain the consent of the patient, either because of physical incapability, such as unconsciousness, or legal incapacity. If the latter is the case, it must also be impossible to obtain the consent of the person legally qualified to consent for the patient.

Good Samaritan Legislation

The Good Samaritan Legislation focuses on the emergency situation that is thrust upon the individual when not at work. Such situations might include the car accident while you are on vacation or the person next to you in a restaurant choking.

In Canada, under Common Law, there is no legal obligation to rescue or assist a person in trouble. The obligation is of a moral or humanitarian one naturally. Good Samaritan Legislation is intended to encourage people to volunteer emergency assistance without fear of liability unless "gross negligence" occurs. Gross negligence could be defined as a standard of care well below the reasonably expected standard due to the circumstances. The law recognizes that a professional who stops to assist at a roadside accident does not usually have his usual "tools" and thus the expected standard of care is modified under the circumstances. Common law holds the caregiver to that standard of care expected of a similar person of similar training and experience in similar circumstances. A good rule of thumb is to only provide first-aid measures to the skill level that you are presently certified. Many first-aid students have expressed concern over being sued for negligence or a wrongful act during an attempt to save a life. If you follow the above rule of thumb, repercussions will be few and far between. For example, if you were assisting a person who was choking, you

would follow your first-aid protocols and make your attempt to assist, but you would not take a knife and perform a tracheotomy.

The person providing assistance in an emergency does, however, have an obligation (duty of care) to carry through any assistance initiated. One cannot begin to rescue a victim and then stop.

Roles of Security/Emergency Medical Responder

Corporations today expect and depend on their security staff to be effective during stressful situations. To be an effective officer, you must acquire a firm grasp of legalities, roles, and responsibilities, and develop the ability to differentiate between legal and medical concerns and act accordingly. Consider the following list of humanitarian duties for the responding officer:

1. Primary responsibility for the safety of the patient.
2. The administering of life-saving care and treatment.
3. Ensure comfort and emotional well being of the patient.
4. Maintain respect for the patient's privacy.
5. Maintain respect for human behavior and religious beliefs.

With regard to different aspects of the role of the security/emergency medical responder, there are other responsibilities which include

Safety: Ensure safety at all times of yourself, the patient, public, and coworkers in the environment.

Confidentiality: In order to respect the privacy of a patient, all matters must be kept confidential and only pertinent information given to the appropriate authorities. Confidentiality must always be strictly adhered to, both on and off the job.

In the event of an on-site disaster, the responding officer may have to assume two identities. During an emergency medical response, you may also be required to perform a variety of security skills such as traffic control, crowd management, scene and evidence protection, note taking and report writing, human relations, security awareness, considering legal and ethical matters, and keeping management apprized of the situation.

Conduct and Attitude

The manner in which a security/emergency medical responder conducts himself/herself and cares for a patient may be as important as the emergency care measures. Try to develop a working rapport with the patient(s), maintain a professional attitude, and demonstrate empathy to put the patient at ease. Remember, nothing sounds as good as "you'll be ok" when you are injured or frightened. A simple gesture, such as touching the patient's shoulder when addressing them, will instill trust and enhance responder/patient communication. Apathy, on the other hand, can quickly destroy all patient cooperation, your personal reputation as a caregiver, and your security department's reputation overall. Emergency medical providers should, therefore, attempt to follow these behavior guidelines:

1. Always try to maintain control even though the scene around you may be chaotic. A confident and professional manner will be transmitted to the patient and may help to alleviate anxiety and fear.
2. Conversation should be kept as neutral as possible and should provide constant reassurance to the patient that everything possible is being done for him/her.
3. Be aware that bystanders and coworkers may also need reassurance during a crisis.

Departmental Training

Unfortunately, there are security/emergency medical professionals who attain their accreditation in their chosen field and then become complacent. Remember that when you achieve your C.P.O. or E.M.S. status, you have just begun your professional training. The three key words are Train! Train! and Retrain!

The sharpest knife will eventually lose its edge if it is not resharpened occasionally. Security departments must continually practice their required skills to maintain an edge. Security and emergency medical response skills must become automatic and second nature if you are to be effective in the field. The time to read the manual is now—not during a crisis situation. There are many varied pieces of rescue equipment involved in security and emergency medical response work. Being familiar with the technology is essential to any successful rescue operation.

One interesting method of maintaining security officers' emergency medical response knowledge is to encourage the officers to volunteer at the local ambulance service. The training they receive will be to local, state, or provincial standards and practical experience in emergency medical skills. The benefits received are compounded both for the officer and the security department as a whole. A working relationship between the security department and the local hospital will be firmly established enhancing professional credibility. The hospital will have greater confidence in the corporate security department if the hospital is involved in ongoing emergency medical response officer training. The security officers will seem to be more than just dominant figures at the local "Company." This kind of exposure will definitely strengthen the relationships between the security department and the townsfolk. As the security officer responds to medical emergencies, he/she will demonstrate community spirit.

Another way to maintain the skill level of the security department is to have the security officers teach first aid and CPR to the employees. Most corporations today sponsor an ongoing first-aid program for employees and sometimes their spouses. This is an excellent opportunity for security and the workforce to meet and develop a mutual understanding and appreciation of their individual roles within the company.

Time should be set aside during staff meetings to discuss security/emergency medical situations that could develop within your organization. This will give each member of the security team a chance to visualize on-site scenarios and related problem solving. Disasters are not predictable, but responses must be. To reiterate, Train, Train, and Retrain!!

Conclusion

The responsibility to attain professional credibility lies with each security officer. As the responsibilities of security departments increase and security professionals are required to handle situations that were previously dealt with by outside personnel, it becomes most imperative that security officers expand their capabilities. If our profession is to achieve and maintain the standards we are setting for ourselves, we must continually strive to improve our skills and meet corporate expectations through continuing education and training.

Security and emergency response are now considered to be related professions. Can you imagine a more fulfilling and important challenge than being responsible for the life of an injured employee?

Security and Medical Response

Quiz

1. First aid may be defined as the temporary care of the _____ and injured.
2. The competency of all emergency medicine _____ has come under close examination.
3. A person may be _____ into medical treatment if they do not want it.
4. Ensure the safety at all times of _____ the patient, public, and coworkers in the environment.
5. Be aware that _____ and coworkers may also need reassurance during a crisis.
6. Cross-contamination of diseases such as AIDS, tuberculosis, and Hepatitis B can be prevented by the use of proper safeguarding techniques. ☐ T ☐ F

7. If a workman is injured with a broken arm, he is obligated to let you begin first aid because you are a security/emergency medical responder. ☐ T ☐ F
8. The Good Samaritan Legislation allows a person to take whatever measures necessary in order to save a person's life. ☐ T ☐ F
9. Once you achieve any certification, retraining is not necessary because you will always be competent in your level of skill. ☐ T ☐ F
10. Confidentiality only applies to you while you work. ☐ T ☐ F

9 Outsourcing in Security

Christopher A. Hertig and Rolland G. Watson

It is not unusual for a private company or governmental organization to outsource services, including security services. This is not a new arrangement; there were probably types of contract security services in colonial America, but it is becoming more common. The term "outsourcing" refers to a staffing method whereby the client organization hires another entity that, in exchange for a fee, provides a service. In the security field, that entity is usually a contract guard service that provides a set number of guard man-hours to a client. In most cases a flat fee is charged, although fee structure can be modified if overtime hours are ordered or special services (strike coverage, armed officers, additional supervision, etc.) requested. Contracting out, or outsourcing, makes good management sense when one of the following criteria is met:

1. The client cannot perform the service for themselves due to lack of expertise, logistical, cost, or legal restrictions.
2. The service is temporary or unusual in nature.
3. Personnel costs (wages, benefits, taxes, etc.) make the service prohibitively expensive for the client organization.

There are many examples of situations where contracting out security service is logical:

1. Nuclear power plants where refueling and repair periods require greater access control, in the form of increased guard posts, due to additional workers onsite with more access points open.
2. Construction projects that require traffic control, fire watch, and theft prevention.
3. Stadiums, concerts, colleges, or high schools that host public events and need crowd and traffic control.
4. Autograph sessions, auctions, stockholder meetings, Christmas sales at retail stores, and film debuts that call for increased security and public contact.
5. Strikes, rallies, and demonstrations that mandate surveillance, crowd, and traffic control.
6. Jewelry stores that need off premises alarm monitoring to meet insurance carrier requirements.
7. Commercial central alarm stations that subcontract alarm response through a local contract security company for their clients.
8. Industrial plants that need supplemental security coverage to cover for in-house guards during vacation.
9. Political figures, business VIPs, or entertainment celebrities that require protection from overzealous spectators while in transit or after receiving sudden, unexpected threats.
10. Payrolls or bank deposits transported by armored car firms.
11. Emergencies such as fires or floods where a facility must be guarded, persons escorted, or assets recovered.
12. War zones where specialized contractors with military training provide executive protection, infrastructure protection, and armed escorts.

13. High crime areas that need to be brought under control. These can be apartment complexes, parks, or shopping centers.

Sometime during your career as a security supervisor of a proprietary guard force or protection specialty unit, your corporation might consider outsourcing. Downsizing or decascading reduces cash flow and improves profitability in the short term.

If your employer is considering such a change, you should be thoroughly familiar with all aspects of outsourcing. Should you be tasked to make a recommendation, you should be ready to answer whether such a move would be good for the corporation as a whole. You should be able to explain, demonstrate, or provide a cost–benefit analysis either for or against outsourcing.

If the answer is yes, you must know what steps should be taken to ensure the services provided are the best ones you can find for the money. Just because a corporation has decided to outsource security does not mean that they are willing to settle for inferior services.

Your officers, of course, hope that you, as their representative, can take an approach that can save their jobs, but that might not always be the best solution for your company. If you fail to retain your force, your job is going to change; if you retain your force, you may have to work more efficiently. No matter what the approach, you will have your job cut out for you. You must be sure that you have all costs, pros and cons, and other specifics for both types of services.

If your corporation decides to outsource, you may have to decide if taking a position with the outsourcing firm would be a good career move for you. Again, you must be armed with the facts to make a good choice for your future.

Pros and Cons of Outsourcing

Advantages to contracting out for security services include:

1. Lower cost due to flat billing rate as opposed to incurring wages and attendant labor costs (30% above the wage cost).
2. Administrative streamlining where the client firm only has to pay the bills and make sure they are getting the service they require.
3. Flexibility of manpower if needs change on a temporary basis.
4. Ease of removing undesirable employees. All that clients need to do is request that they not be assigned to their account any longer.
5. Elimination/preclusion of guard unions. This has been a traditional selling point; of late, however, there have been substantial movements to unionize contract forces. Generally large, stable security forces face the prospect of being unionized.
6. Ease of rule enforcement due to the outside, independent nature of the security force.
7. Reduction of liability due to independent contractor rule. While this does not always afford protection, a true independent contractor relationship does just that.

Disadvantages of having a contract guard service include:

1. Lower quality of personnel who make inferior wages.
2. Lower loyalty of personnel.
3. Lack of control due to putting in another layer of management via the contract firm. Asset protection is an integral management function that may not be properly outsourced in all circumstances.
4. Poor liaison with law enforcement, which does not want to work with unprofessional personnel
5. Liability protection is almost always absent due to the client directing and ratifying contractor conduct, strict liability, intentional torts, and nondelegable duties. Perhaps more important, having a contractor involved creates an additional target for a plaintiff's lawyers. It makes it easy for them to "divide and conquer" where the contractor and client are fighting with each other in court. This is a complex issue with many variables!

The advantages of hiring off-duty police as contract security include:

1. High caliber, professionally screened personnel.
2. Well-trained, experienced officers used to handling a diverse range of situations.
3. Increased investigative capability due to training, experience, and access to official database.
4. Improved liaison with local law enforcement agencies.
5. The ability to have armed personnel where legal restrictions may make this capacity unattainable.
6. Possible utilization of public resources such as vehicles, radios, investigative equipment, etc.
7. Arrest authority possessed by police can aid in dealing with troublemakers.
8. Greater deterrent to crime—at least this is commonly believed to be the case.

Disadvantages to using off-duty police include:

1. Police react to, rather than prevent problems. They may not be attuned to security services and all that that entails. A community policing philosophy will help to make them more proactive.
2. Training/socialization may lead them to be abrasive and/or brutal. This may occur with urban police departments.
3. Lack of a customer service ethic or client orientation.
4. Conflict of interest between public and private role in crime control.
5. Conflict of interest regarding restricted information. This can be a substantial issue.
6. Police may see their secondary employment as unimportant. This can be a serious service and safety concern. Officers who think of their security job as "just standing around in a _____" are creating the recipe for disaster.
7. Costs may be high, and there is really no competition. Costs for off-duty police are higher than any other type of protection. Unfortunately this cost is likely to escalate.
8. Legal issues may arise due to the interests that officers were acting to further. This needs to be thoroughly assessed before the officers are deployed.
9. Control over the officers and the ability to terminate the contract is severely limited—clients may fear future reductions in police response time if officers are removed.
10. Possible illegalities involved due to tax laws, private detective statutes, etc. These must all be researched fully prior to signing any contracts. Cutting corners can create major problems in the event of a civil suit.

The advantages to contracting out alarm monitoring include:

1. Costs, especially start-up expenses, are minimized.
2. Maintenance and monitoring with all of the associated labor costs/concerns are eliminated.
3. Insurance company requirements are met and premium reductions obtained.
4. Off-site storage and management of alarm information provide some additional protection in the event of a disaster.
5. Administrative streamlining of alarm monitoring and response functions and easier budgeting.

Disadvantages of contract central alarm stations include:

1. Possible delays in obtaining alarm activity information.
2. Extra charges for monitoring, response (in some cases), and dedicated lines.
3. Lack of control over contractor personnel management.
4. Unfamiliarity of central station personnel with alarm points or areas. If operators don't physically visit the site or go to the appropriate screens, they can't properly assess what is happening when an alarm annunciates.

When Outsourcing is Inevitable

Your job is far from complete after the decision to outsource is made. You will become involved in conducting an outsource security survey and the contracting process. These are not to be taken lightly as they will require all your management and human relations skills to ensure your organization has the best security that can be obtained at a price that is affordable. The selection and contracting process will consume time that would ordinarily be spent in your function as a supervisor—plan on alternatives for completing your day-to-day job.

Every organization wants quality at the most affordable price. Who will be responsible for obtaining and contracting for that quality? You will! The service will be what you make it. With that in mind, let's look at some fundamentals of determining cost.

Determining Cost

There are several factors that must be included when costs are determined and each identified factor is as important as the next. You should:

1. Conduct a thorough cost–benefit analysis of both your proprietary service and anticipated contract service.
2. Identify liability issues and costs. Consult with the supplier of your organization's current liability policy for your proprietary force. Determine your present costs and what you will save by outsourcing. In some cases, depending on the type of business, there won't be savings. Financial institutions, for example, have a blanket liability policy that covers your proprietary force at no additional cost.
3. Determine liability coverage and cost for:
   a. Armed proprietary.
   b. Armed contract.
   c. Unarmed proprietary.
   d. Unarmed contract.
4. Quantify wages and benefits. How do you compensate your proprietary force? What is the cost of your organizational benefit package? Traditionally, a benefit package may be 14–41% in addition to salary. In outsourcing, you should identify:
   a. Current salary and benefits.
   b. Locality scales in relationship to benefits and salary.
   c. Incremental longevity proprietary scales.
   d. Contract cost per hour versus salary per hour.
   e. Contract benefits.
   f. Compare and contrast after-analysis retention and turnover rates between proprietary and contract. It is not unheard of for some contract security forces to experience a turnover rate of over 200% per year. Will your directors, suppliers, and customers tolerate a turnover rate of that proportion? Remember that retention levels can be made part of the contract.
5. Provisions—uniforms and equipment. A proprietary force is normally equipped by the organization with uniforms, radios, equipment, office space, phones, etc. When you outsource, you need to identify:
   a. Cost of organization property to be transferred.
   b. Who will be charged for maintenance or replacement?
   c. How will telephone bills, lost equipment, or breakage be recovered?
   d. Key and inventory control processes. Who pays if locks or equipment must be replaced?
   e. Will the contractor be required to purchase on-hand supplies and materials as a condition of the contract?

These are just a few of the questions that need to be answered when you conduct your cost–benefit analysis in provisions, uniforms, and equipment.

6. Other headaches that can occur are:
   a. Who owns the firearms carried by the guards?

   b. Must the organization maintain an armory?
   c. What happens to patrol vehicles?
   d. Who provides weapons and vehicle training?
   e. How often must officers qualify with firearms and safe driving requirements?
7. Training issues. A major liability issue in security services is training. Many supervisors and corporations are being sued today under the theory of "failure to train." When you have a proprietary or contract guard service, the organization, the contract service, and all the security supervisors, directors, or managers are both corporately and individually liable if they know, allow, or fail to provide training that any reasonable person would conclude was a responsibility of that entity or person. What types of training will you require to maintain the high image of your corporation? These requirements and costs must be included in the contract as an expense borne by the contractor. This training will need to be documented and proof retained by the contract manager. Training is normally accomplished to some standard set out in the service provider's job description. In security service, some training issues are:
   a. Use of force.
   b. Use of deadly force or drawing the handgun.
   c. Protection of people, organizational assets, and the protection officer individually.
   d. Physical fitness, deportment, and conduct.
   e. Police involvements and conduct prejudicial to organizational standards.
   f. Emergency procedures.
   g. Customer, client, community, or public relations.

Without a comprehensive list of training requirements, a failure to accomplish a task or duty could have severe liability issues for the organization and contract company. It is your job to identify training needs and to ensure they are specified in the contract and are conducted and documented. Contractors with quality corporate training capabilities should be given more consideration than those without them.

Other issues to be considered are:

1. Identify the strengths and weaknesses of proprietary and contract services.
2. Create a matrix or checklist that delineates both positive and negative attributes of proprietary and contract security services. Itemize the list to provide a total comparison of both services. Ensure you include:
   a. Current costs.
   b. Projected costs based on inflation or contractual raises.
   c. Training costs.
   d. Liability costs.
   e. Recruitment, retention, and screening costs.
   f. Costs of having to cancel a contract with one firm and replace them with another firm, a proprietary force or off-duty police.

There are some costs that are intangible but should be entered into the matrix: loyalty, dependability, honesty, integrity, and commitment to the organization. These intangibles may cost you more money when outsourced.

Soliciting the Contract Bid

You should create a detailed specification sheet for the outsourced positions and duties for which you want to contract. Develop a list of current reputable contract services in your area and mail them a solicitation to bid on your contract. In some cases, a highly detailed request for proposal is developed that specifies your requirements. Unfortunately, having an impressive list of specifications may entice service providers to embellish and exaggerate their capabilities. It may be better to simply ask via a letter for a proposal, giving the vendor some key points that must be met. Check national publications and state licensing authorities for additional companies to contract. Hold face-to-face interviews, and check with other corporations in your area to see who they use, and if they are satisfied. Then, check with

your local law enforcement agencies to see which companies they have the best rapport with. Go and observe the prospective contractor (this process is akin to a background investigation on an employee where references and prior employment history are assessed). Do not use companies that have poorly maintained vehicles and sloppy security officers. Does the prospective contractor reflect your corporate image? Remember that low bid usually always means low service. From an operational and service quality perspective, "low bid means no bid"! Unfortunately, cost savings may be the key concern to some decision makers in your employer's management team. Make certain to carefully document all aspects of your research into contract firms.

Writing the Contract

Your contract must be specific in its requirements—nothing should be left to the imagination or speculation of either party. You need to include such things as initial and ongoing training requirements, and who will oversee your contract, hours of coverage, uniforms, equipment, and related costs. What will the contract cost be on an hourly basis, and what will the guards earn in wages and benefits on an hourly basis? Will the guards receive periodic wage increases, uniform allowances, or paid vacation? Who will be responsible for liability costs? Make sure that your corporation is covered under the contractor's liability. Include a place for your present proprietary officers to retain their positions with the new contract.

What will the Role of Security Be?

This must be clearly delineated in the contract and must be completely and clearly listed so that there is no doubt what security will do and what is expected of each and every contract guard. The four Cs of contracting are:

Clear—precise language articulates what is intended
Concise—to the point, avoid long sentences, and flowery phrases
Correct—ensure that the contract states specifically what is expected; allow no mistakes
Complete—all aspects of the relationship are covered; nothing is left out
Make sure you have covered all the bases for your organization or you may be looking for work elsewhere. The role of the security department and its personnel is pivotal in the contracting business.

Contractor Evaluation Checklist: Selecting the Contractor

Create a numbered checklist for each item you want included in the contract and then check each item to ensure compliance. The number or sequencing should be systematic and complete while maintaining an ease of use. Be sure you include all of the items mentioned in this article and any other items important to your organization. Also include such things as branch support, field support and personnel, experience in security (not law enforcement), selection, knowledge, and professionalism of the contract company representatives. Using this system as a grade, you will be able to determine which contract company matches your requirements.

Your Continuing Role in the New Program

Finally, it is important that you determine what your role will be in your organizations new or revised security program. If you are retained to oversee the contract, then you must obtain additional training. Expand your duties to include life safety, risk management, investigations, and executive protection. If your corporation has decided to outsource your position, then you must make sure you have seen to it that you have included a place with the contractor for yourself. Keep in mind that you are not alone in this. Many other security supervisors have had the same task assigned to them. Besides being able to consult with the other security supervisors in your area, there are many sources available to assist you in this process.

Contract security offers people extensive career advancement options. Consider that contract security may be entered into on a part-time basis while in college or the military. Many of these jobs can easily suit one's schedule. Many are very challenging and interesting. Also, consider

that contract security performs an ever expanding series of functions. Historically where there has been a market, security service firms have evolved to meet the demand. Realize also that contract security is unlike other security, law enforcement, or military functions. One must understand the culture of how it operates and interfaces with the clients in order to succeed within it. Due to this, security service generally promote from within. The corporate ladder is extensive in contract security. Career success in contract security can be obtained by:

1. Taking human resources management courses and developing expertise in this area. Most of the daily operational issues in contract security involve recruitment, selection, scheduling, and payroll. Competent supervisory and managerial personnel must be knowledgeable of the HR process. They must also master the hiring, training, and motivation of personnel in order to provide quick, efficient service on demand.
2. Studying sales techniques and client relations so that contracts can be obtained—and maintained! While not all service firm providers are sales reps, meeting with current and prospective clients is a key function shared periodically by all management personnel.
3. Becoming thoroughly conversant with state and local laws that govern contract security services providers. This includes licensing and training requirements. It also encompasses employment laws such as wage and hour laws, Civil Rights Protection Acts, etc.
4. Being knowledgeable about the business that the client firm is in. This enables the contractor to provide higher level of service. Some successful firms specialize in particular market sectors (nuclear, healthcare, shopping center, etc.). They also have specialized training programs for their personnel so that they are competent within the particular vertical market to which they are assigned.
5. Being able to obtain technical expertise for investigations, security assessments, etc., when needed. Years ago, few people in contract security had any real technical expertise. This has changed! The need for this knowledge arises periodically. Smart service providers can deliver it to a client in short order. One simple consideration is the number of management and line staff who are professionally certified. This provides insight into what the firm really thinks about professional growth and development. It separates those companies who merely "talk-the-talk" from those who actually walk-the-walk."
6. Networking in professional organizations, such as the National Burglar and Fire Alarm Association, ASIS, etc. This networking provides insight on industry trends and facilitates more productive relations with clients and employers.
7. Being licensed to carry weapons, conduct investigations, or becoming certified as an instructor are also useful in the security service field. The need for armed personnel or investigators may or may not be constant, but sooner or later a potential client will need these services. Additionally, being able to instruct in accordance with state or provincial laws or company standards (Crisis Prevention Institute, Pressure Point Control Techniques, etc.) can give a practitioner added value.

For More Information

The British Security Industry Association (bsia.co.uk) works to establish training standards, disseminates information about the industry, and effects legislative liaison with governments.

The Confederation of European Security Services (coess.org) endeavors to represent the collective interests of contract security firms in Europe. The Confederation also collects and disseminates information on the security industry.

The International Association of Security and Investigative Regulators (www.iasir.org) is an organization of those personnel who train, regulate, and license investigators and security service firms. Members represent state and provincial regulatory entities throughout the United States and Canada. IASIR provides a link between licensees and government regulatory agencies as well as end users of security and investigative services.

The National Association of Security Companies (NASCO) (nasco.org) is a professional organization of contract security firms. NASCO works within the contract security industry through legislative initiatives, information sharing, and liaison with other professional organizations. The association publishes a magazine, has a recruitment section on its website, and offers various other services to its members.

The Private Security Services Council of ASIS International (asisonline.org) promotes the exchange of information among providers of security equipment and services.

An online tutorial about contract security is available at ifpo.org. It may also be accessed through the York College of Pennsylvania site at ycp.edu; go to the Contact Directory and see the Web site for Professor Hertig. The tutorial is a study aid for persons in the Security Supervision and Management Program.

Outsourcing in Security

Quiz

1. Contracting out, or outsourcing, makes good management sense when one of the following criteria is met: (select best answer)
   a) The client cannot perform the service for themselves due to lack of expertise, logistical, cost, or legal restrictions.
   b) The service is temporary or unusual in nature.
   c) Personnel costs (wages, benefits, taxes, etc.) make the service prohibitively expensive for the client organizations.
   d) All of the above.

2. Administrative streamlining, where the client firms only have to pay the bills and make sure they are getting the service they require, is an advantage to contracting out the security services. ☐ T ☐ F

3. Another form of contract security is to hire _____ duty _____.

4. Taking _____ courses and developing expertise in this area may add to career success in contract security.

5. Asset management is an integral management function that may not be properly outsourced in all circumstances. ☐ T ☐ F

6. It's very difficult to remove undesirable employees in a contract situation. ☐ T ☐ F

7. The 4 "C" of contracting are: _____, _____, _____, _____.

8. Make sure to thoroughly document all of your _____ involving prospective contract firms being considered.

9. When writing the contract, you will not be able to mandate wages and benefits for contract guards. ☐ T ☐ F

10. In using a contract security company, you have no choice in officers. ☐ T ☐ F

10 Internal Loss

Christopher A. Hertig, Robert Metscher, and Whitney D. Gunter

Introduction

An understanding of internal loss is essential to anyone involved in "Asset Protection." Internal theft has been the traditional, and in some cases, sole focus of inquiry. Contemporary study must include sabotage, threatening/harassing behavior, loss of productive time, and theft of protected information (proprietary, confidential, or classified). These loss streams can cost an organization a tremendous amount; in some cases threatening the very survival of the business. The total cost of loss must be taken into consideration as direct losses; the cost of replacing the property, time, or property lost can be extensive. Indirect losses such as lowered morale due to coworker resentment of dishonest employees taking unfair advantage of their positions are substantial. Extra expense losses such as extensive audits of computer programs following sabotage or theft or the increased advertising in the wake of an embezzlement scandal can be astronomical.

Scope of the Problem

Both practitioners and researchers agree that internal theft is an extensive source of loss to corporations. Tyska and Fennelly (1998) state that 25% of all employees will steal from their employers if the opportunity presents itself. Lary (1989) cites a 1983 U.S. Department of Commerce study, which concluded that one third of all employees steal from their employers. Other studies state that 40% of the workforce is inherently honest with 30% willing to steal and the remaining 30% capable of stealing if the conditions are right (Lary, 1989). Horan (1997) takes a more cynical view with his mention of a standard rule of thumb that 10% of employees will never steal, 10% will always steal, and 80%, often referred to as "fenceriders," may steal.

Estimates are that 30% of business failures are due to internal theft (Lary, 1989; Tyska and Fennelly, 1998). In a 1985 study by the Stanton Corporation, it was found that 32% of job applicants admitted stealing from a previous employer (Lary, 1989).

Additionally, it appears that internal losses are compounded by dishonest employees. There is a "rolling-ball effect" similar to the "broken windows" phenomena relating to street crime and disorder. Employee deviance leads to more dishonesty, a deterioration of productivity, and increased customer dissatisfaction (Tyska and Fennelly, 1998). Horan (1997) maintains that auditors who find deficiencies in physical security are certain to find compliance problems such as in cash handling. James Walls, senior vice president of the Stanton Corporation, an honesty testing firm, maintains that the amount initially admitted to being stolen can safely be multiplied 10-fold (Lary, 1989). This is evidence of the principle of expansile significance.

Clearly, there is substantial loss in American corporations. Assessing the precise extent of that loss is difficult. Research limitations are inherent due to the confidentiality with which many employers handle thieves. The "private justice system" is not easily studied.

Models of Internal Loss Causation

Beginning with the work of Edwin Sutherland, there has been some criminological research into white collar crime and embezzlement. Some of this has been undertaken by criminologists, such as Sutherland's protégé Donald R. Cressey, who wrote the seminal study on embezzlement, while other portions have been addressed by scholars in the "accounting profession."

Unfortunately, these models are limited to internal theft. Contemporary Personnel Security must address such topics as workplace violence, threatening behavior, theft of information, and sabotage of computer systems. Hopefully future scholars will develop models that focus on these problems as well.

Cressey (1953) has used a formula for employee theft, which is:

Motivation + Opportunity + Rationalization = Theft

Motivation arises from a real or perceived need for money; often an "unshareable need" such as a gambling debt.
Opportunity can occur any time the criminal has access to an asset such as cash. Failure to separate functions and put appropriate supervisory systems into place create opportunity.
Rationalization may include such things as the feeling they are underpaid or that the employer owes it to them or that they are merely borrowing the money.

Which theory or theories of crime causation does the Cressey formula relate to most closely?

An accounting professor, Dr. W. Steve Albrecht, cited by Lary (1989) devised a similar model:

Motive + Opportunity + Personal Integrity = Theft

Motive—often arising from personal financial pressures. Horan (1997) mentions a standard rule of thumb, which postulates that 10% of employees will never steal, 10% will always steal, and 80% will steal if they are allowed to. Periodic evaluation of an employee's lifestyle can enable management to build a profile of employee need.
Opportunity—lack of accounting controls.
Personal Integrity—degree to which a person can resist temptation; every person will be dishonest in certain situations if the financial pressure and perceived opportunity are great enough. Rationalization will erode personal integrity in these situations. Horan (1997) postulates that there are two basic rationalizations for theft in the workplace:

They won't know if it's gone.

They don't care if it's gone.

Which theory or theories does the Albrecht model most closely correspond to?

Fishman (2000) maintains that there are three elements necessary for an employee theft to occur:

1. A *motivation* to steal: This may come from a need for more money to support a lifestyle, pay for a medical or other emergency or holding the belief that the employer owes them more than they are being paid.
2. An *opportunity* to steal: Opportunity relates to the "least effort principle" or rational choice theories in that an unsecured asset will not deter an employee from stealing it (Nalla and Newman, 1990).
3. A *belief by the thief that there is a way to hide the theft* and avoid detection: This may arise from a lack of internal controls and the separation of functions. Traditionally, a decision maker (one who authorizes a purchase or payment) is separated from the employee who has custody of the account and is responsible for it. An accountant has neither the authority to authorize use of the account (or other asset) nor custody and control of it. The accountant is responsible for maintaining records of the account. In some work environments, this separation

does not exist due to the cost of personnel or the integration of computerized accounting. In these types of environments, theft may not be detected easily.

Nalla and Newman (1990) discuss the "Choice-Structuring Properties of Crime":

1. Attraction: How attractive the target asset is to the criminal is one factor in determining whether a crime will be committed.
2. Access and availability of the target to the potential criminal.
3. Complexity required to carry out the crime in terms of planning and logistics.
4. Moral climate in the workplace, which may make it easier or more difficult for the criminal to justify the criminal act.
5. Risk: The chances of getting caught are assessed by the criminal candidate.

How does this model relate to those of others?

There are undoubtedly employees motivated by vengeance against their employer. Again, models of internal theft must be expanded to include vengeance, internal psychological stress, and other motivating factors for workplace crime.

Types of Crime and Loss

While the traditional treatment of internal theft has been to focus solely on misappropriation of assets, the scope of the internal loss problem is much more complex. Personnel security issues include the threat of sabotage, theft or dissemination of information, harassment and threatening behavior, etc. The use of Bottom and Kostanoski's WAECUP Model can aid in an expanded exploration of these issues.

W—Wasted space may be used for illicit activities such as sleeping, gambling, or substance abuse. Waste containers may be used to get items out of a facility by employees who put things in them and either retrieve them later or have a confederate do so. Waste containers should not be accessible to outsiders who may do some "dumpster diving" in order to retrieve valuable information.
Inappropriate waste management can contribute to useable items being discarded—in some cases items or materials that are not needed at a facility could be sold or given to a charitable organization—not doing this wastes an opportunity to perform valuable community service and obtain positive public relations!
Wasted time is probably the greatest loss contributor; taking forms such as "goldbricking," chatting via email, Web site browsing of nonwork-related sites or the inappropriate assignment of tasks so that some employees don't have enough to do.
A—Accidents may be used to cover up theft—in some cases employees will intentionally damage items so that they can take them home in accordance with policy. Accidents may also be fraudulent or exaggerated in terms of injuries whereby employees file workman's compensation claims. A questionable accident may well be an illicit attempt at getting a "paid vacation" courtesy of workman's compensation insurance.
E—Errors in accounting or inventory may result in loss or they may indicate theft that really isn't theft. Having people checking each other's work is essential. Layers of audits must be in place to minimize the chance of errors.
C—Crime may be internal theft such as embezzlement or pilferage, or the theft of time (time-card cheating), unauthorized discounts or refunds, or the selling of information. Sabotage, vandalism, harassment, and even arson and bombings may occur. These latter actions may increase in frequency during a labor negotiation or downsizing.
Unethical/Unprofessional Practices—Kickbacks or the selling of information may occur. There may also be harassment, threats, or stalking behaviors, which fall short of being criminal violations. These latter are rather extreme forms of unethical practices; more common practices include:

- Abuse of sick time
- Fudging of time sheets
- Taking longer breaks than authorized

- Arriving late and leaving early
- Deliberately working slower and less efficiently
- Working while under the influence of alcohol
- Abusing employer resources such as telephones, copy machines, and computers
- Tending to personal business while working

"Broken windows" theory or the "rolling-ball effect" may occur in workplace cultures where there is mass dissatisfaction. "Toxic workplaces," where employees are required to choose between a life and a career, are treated as a factor of production rather than individuals and when employees are seen by the employer in terms of the costs they represent also may be ripe for internal theft and loss. Inadequate pay, benefits, job security, promotional opportunities or ambiguity in job roles, relationships, and responsibilities all contribute to internal loss. Clearly, employees in poorly managed workplaces can pilfer small amounts on a continuous basis and systematically destroy a substantial amount of goods and materials out of sheer vengeance. While such actions are inherently wrong, management has an ethical obligation to its employees not to "use and abuse" them. Setting a positive ethical example and managing morale within a work environment are crucial to stemming losses due to unethical/unprofessional practices.

Good management is good security.

Cultural Factors

The prevailing workplace culture will determine to some extent which type of crime a workplace is exposed to. Individuals seeking careers in Asset Protection Management must be able to read a particular organization's cultural characteristics; they must be "industrial anthropologists" to some extent.

Nalla and Newman (1990) define the following types of workplace cultures:

- Tough guy—fast paced, entrepreneurial, risk-taking for fast, short-term gains such as in publishing, commodities dealing, etc.
- Bet your company—high risk over the long-term through investing in the development of new products, services, formulas, etc.
- Work hard/play hard—constant pressure to produce revenue and increase market share is present. Less risk, more emphasis on customer service, and long-term gains.
- Process—a bureaucratic environment where there is little risk and often heavy government regulation. Employees have long tenure and the work environment is predictable.

Prevention

Prevention of internal loss can be divided into three major areas: employee screening (vetting), employee socialization, and internal controls.

Employee Screening

Screening of employees is an essential component of the personnel security process. Job applications should be verified. Interviews should be conducted to assess employee honesty. Honesty tests may be given. In certain cases, polygraph tests may be administered. Drug tests are a simple method of weeding out undesirable employees. Background investigations—driven by the information on the application—need to be conducted.

Employee Socialization

Beginning with recruitment, employees are socialized into the organization. They learn organizational rules, values, as well as specific job functions. The socialization process includes every phase of the employment relationship from recruitment, to selection, to training, and to discipline. "Messages" are given to the employee at each juncture, both through the formal organizational hierarchy and the informal employee network.

Internal Controls

This includes access control and the separation of functions. Also, "dual-control" may be used to perform certain critical functions. This technique is common in high-security environments.

Security Awareness

Modifying employee attitudes and subsequent behaviors is an essential element in socializing employees so as to control losses. Security awareness programs are often used to combat theft and information loss. These programs can be used for safety awareness; in fact they probably have more extensive implementation within the safety arena than in combating internal theft and information loss (this may be due in part to the aggressive role of insurance carriers as well as the extensive amount of laws regulating safety).

An additional benefit of reducing internal loss—often seen in the counterintelligence effort—is that employees who are more aware will report loss causing situations that arouse their suspicions. Early identification of potential problem areas is critical to the taking of preemptive actions. This may be more critical with embezzlement and intelligence probes as these activities are concerted, concealed, and take place over a long period of time. In many cases, they go undetected until an unusual event occurs that uncovers the scheme. Employees being critically observant may reduce the time lag between instigation and detection to a considerable degree.

Awareness programs can begin with employee orientation. They must continue throughout the employment relationship. Beginning with employee orientation and ending with exit interviews, astute managers can engineer an array of communication opportunities to "get the message across."

Awareness through the spoken word can take place in many forms including "house organs" (employer newsletters), paycheck messages, Web site information, specific newsletter dedicated to safety and/or security issues, signage, and posters. Horan (1997) advocates putting in references to honesty and integrity in the Mission Statement. Ideally, there should be references to honesty and integrity in the classified ad. The application process should impress on the job seeker that the employer is going to conduct a thorough background investigation.

Awareness programs are not automatically effective. There are probably many programs that have little or no effect on internal loss due to their inadequate design and/or execution. One can review crime prevention programs sponsored by police departments and see that in some cases they have been staffed with personnel who are no longer able to perform patrol functions due to physical disability, etc. Often crime prevention programs are driven by a desire to maintain positive public/community relations and maintained by all the free handout available from the National Crime Prevention Coalition. In such an operating environment, program effectiveness is rarely assessed.

Tyska and Fennelly (1998) provide some rules of thumb for conducting awareness programs:

- Know the audience.
- Target the right audience.
- Design, develop, conduct, and evaluate programs that are both relevant and effective.
- Presentation skills are important.
- The wheel does not have to be reinvented (p. 13).

Additionally, awareness programs must be backed up with real life examples that the employer is serious about loss control. Upper management's commitment to honesty, the rigor of the selection process, audits that are conducted and the vigor with which irregularities are investigated all make an impression. A true awareness program is built on a foundation of organizational commitment.

Auditing

Audits are checks or verifications that procedures are being followed. They are inspections. They are essential to loss control efforts. Horan (1997, p. 149) reminds us that "the audit function serves to open dialog and provide a training forum for shortage awareness."

In a retail environment, Horan (1997) recommends assessing five elements:

1. The physical security of the location such as CCTV, electronic article surveillance (EAS), locking procedures, etc.
2. Cash control procedures.
3. Procedures such as shipping and receiving personal property brought into the building, etc.
4. The utilization of the point-of-sale (POS) exception report to assess unusual register transactions such as above average numbers of voids, overage, or underage.
5. Overall standards for handling merchandise on the selling floor and in the stock room.

While these elements are oriented to a retail environment, the first three are generic to virtually any type of operation.

Investigation

Investigation of loss events is an essential function for asset protection professionals. Investigation is essential to determine exactly what the loss is, what caused it (errors can easily be mistaken for thefts), and how to reconcile it (confessions, convictions, etc.). Tyska and Fennelly (1998) maintain that there are five methods by which employee dishonesty is detected:

1. Coworker tip-offs
2. Security audits
3. Shopping service
4. Electronic surveillance
5. Exception reports

According to Horan (1997), there are three types of written statements that investigators must become familiar with:

1. *Evidentiary statements*, which document criminal acts and are used in criminal proceedings or labor relations hearings.
2. *Procedural statements*, which document willful violation of company policy that creates the potential for loss and that will be used to support formal disciplinary action against the employee.
3. *Informational statements* given by witnesses of unusual incidents. These are collected as part of the investigative effort.

Protection Officer Role

Security officers have four basic roles within an organization:

1. Management representative: where they are the link between management and employees. Carrying out this role in a diplomatic fashion is essential to the maintenance of positive work relations.
2. Intelligence agent: This is where the officer reports on all unusual conditions or situations, which could create the potential for loss.
3. Enforcement/compliance agent: The protection officer must ensure that management's policies are carried out.
4. Legal consultant: Security personnel must make a whole host of legal determinations such as whether to address something as a policy violation, a civil action, or a criminal matter. Privacy and search and seizure questions are generally part of labor law and are governed by union contract and management policy. Officers must also be familiar with administrative agency regulations such as OSHA, EPA, FCC, etc.

To better appreciate the role of protection officers in internal loss control, the acronym INTERNAL has been developed:

I—Inspect the facility for procedural violations, degradations in the physical security system, and unusual, unexplained conditions.
N—Note all findings of the inspection process. "When in doubt, document."
T—Theft. Understand the elements of theft. These are unique to each state or province. They are also specific to certain types of theft such as embezzlement, theft by deception, or receiving stolen property. In general, elements of theft or larceny are:

1. An unlawful taking
2. Transportation or the carrying away of the property
3. The taker is not the rightful owner or possessor
4. Intent to permanently deprive the owner of the full value of the property

In addition to theft or larceny, the officer must know statutes relating to assault, harassment, computer abuse, vandalism, etc. These are specific to the types of internal loss events that can be reasonably expected to occur in a work environment.

E—Environment. Becoming intimately familiar with one's patrol environment aids immeasurably in determining when something detrimental is occurring.
R—Report all discrepancies and violations of rules. Report both in writing and verbally. Documentation can include notes, logs, daily activity reports, and incident reports. Reinforce the message with a verbal report to the appropriate person(s).
N—Neutrality. Being a detached, neutral, and objective observer is essential to professional handling of workplace deviance. Personal prejudices or preconceived notions have no place in protection or investigative work. "Just the facts." Let the facts speak for themselves.
A—Audit the physical security system such as locking procedures, access to areas, intrusion detection capabilities, safe, vault, and locking file cabinet procedures. Check for information carelessly left unattended on desks, computer screens, or other places. Audit that procedures for receiving shipments are being followed.
L—Loss can be direct, indirect, or extra expense. Effective asset protection professionals have both an understanding of loss potential and an appreciation of how it impacts the organization they are protecting.

Resolution

Internal discipline must be implemented in each and every case of employee theft, abuse, or dissemination of protected information. Clear policies must be developed and disseminated for this to be effective. Also, management must conduct a thorough investigation before enacting disciplinary measures.

Other resolution actions may include:

Contractual agreements signed by employees, which set up a schedule of repayment. This is common in retailing where a premium is placed on interrogation ability: getting the employee to first admit the thefts and the amount stolen is paramount. Next, a repayment plan is developed and signed by the suspect.

Civil recovery—as is most commonly used in shoplifting cases—is available in some states. The employer sends a civil demand letter to the thief who will either pay or face a suit or have a lien placed on his/her property. These letters do not produce results all of the time, but Read Hayes noted retail security expert found that about 40% of the time payment is obtained after the first letter is sent (Zalud, 1988). It may well be that civil recovery will spread for computer-aided thefts and sabotage as corporations are in a much better position to investigate these events than public sector investigators.

Criminal prosecution is standard policy at some organizations where the loss is above a certain amount. It is probably a safe assumption that the number of organizations, who use criminal prosecution for other loss events such as workplace violence, is increasing. Obviously liaison between police, prosecutors, and security departments is very important.

Criminal restitution can be ordered by a court as either a diversionary program whereby the accused is not prosecuted or as part of the sentence. Jurisdictional variations are great; security personnel must be familiar with local policies governing the prosecution of adults and, where applicable, juveniles.

Above all, loss control professionals must remember that the criminal justice system has a role and function, and the management of businesses has a role and function. They are not one and the same.

Career Opportunities

There are rapidly expanding career opportunities for individuals possessing the requisite skill sets in the fight against internal loss. While most of this work is for private organizations, public entities are certainly not immune from the same problems. Individuals with the following skill sets can do well in their careers:

- Interviewing
- Interrogation
- Report writing
- Accounting
- Surveillance
- Data base investigation

Experience, education, professional certification, and state licenses are also important. Making the right contacts with potential employers and clients is *critical*.

Private Investigators

These individuals offer a vast array of investigative services to clients. Most people start their careers in this field doing surveillance for workman's compensation fraud cases or undercover (UC) investigation of workplace irregularities. Private investigators (PIs) also investigate the backgrounds of those being hired or promoted, locate assets owned by persons, conduct surveillance, etc. Some firms specialize in financial investigation relating to theft or fraud.

UC Investigators

These are PIs who are recent college graduates in most cases. It is a common starting point in an investigative career. UC work is one method of obtaining a critical perspective of the social networks within a workplace. Waste, fraud, abuse, theft, substance abuse, and sexual harassment can all be studied through the eyes and ears of an UC operative. With the widespread use of illegal drugs, UC operations often get involved with this.

There are hazards to this work, such as emotional fatigue—one must constantly lie—and physical hazards such as assault by criminals. Pay is excellent as one is paid by both the client and the PI firm. There are also provisions for living expenses, moving expenses, etc. *Preferred job assignments are with established firms who specialize in this type of work.*

One type of "UC" investigation is honesty shopping or shopping service. This is where an agent poses as a customer and makes a purchase. The service can be done to determine honesty, such as purchasing two items of the same price and seeing if the clerk charges the same both times. It can also be done to assess adherence with procedures or customer service. Shopping services are done by specialized private investigation firms as well as some corporate security departments in retail or the restaurant business. See W-Z.COM for more on this.

Retail Loss Prevention

Retailers face tremendous risk of pilferage and organized theft rings by employees. Depending upon the corporate philosophy, some retail loss prevention or asset protection departments hire

agents at the entry level who get actively involved in investigating employee theft. There are considerable opportunities for advancement for those with corporate savvy who do not mind traveling. Compensation packages are excellent, and there are numerous employment opportunities as there are numerous retailers. See LPJOBS.COM for more information on this.

Corporate Investigators

Some corporations have investigators within their asset protection departments. Generally this function is performed by security agents or security supervisors; those organizations with extensive loss problems may have designated investigators who specialize in that field.

Internal Auditors

Internal audit functions are common within businesses. Those with accounting and auditing experience can move into these jobs. An accounting degree or at least significant coursework is expected. Inventory control experience is also an excellent way of moving into this type of work or working within a corporate or retail loss prevention organization. Purpura (1984) discusses the use of teams of investigators, auditors, and computer experts as being necessary to investigate thefts involving a computerized account.

Forensic Accountants

Specialized accountants who can determine where funds have been diverted and seek legal recovery, and/or prosecution are sometimes called in. These people have degrees in accounting, may be Certified Public Accountants (CPAs), and have years of experience in this field. Forensic accountants could work for accounting, investigative, or consulting firms. They may also be employed by government agencies.

Certified Fraud Examiners

This designation was developed by the Association of Certified Fraud Examiners (CFEs) to identify those individuals who have successfully met all selection criteria. The CFE program is a self-paced distance education process culminating in the designation of "CFE." Candidates must study investigation, interviewing, criminology, ethics, accounting, etc. They must also have a requisite amount of education and experience. CFEs recertify with continuing professional education credits each year. Various salary studies have shown that earning the designation increases one's employment and income potential to a significant degree. CFEs work for private investigative firms, corporate security departments, government investigative agencies, district attorneys offices, and accounting firms.

References

S. M. Abassi and K. W. Hollman (2000). Turnover: The real bottom line. *Public Personnel Journal* 29(3).

N. R. Bottom (1998). Employee dishonesty, crime in business. In *Protection Officer Training Manual*, eds. R. R. Minion and S. J. Davies. Woburn, MA: Butterworth-Heinemann.

R. V. Clarke and D. B. Cornish (2001). Rational choice. In *Explaining Criminals and Crime: Essays in Contemporary Criminological Theory*, eds. R. Paternoster and R. Bachman. Los Angeles, CA: Roxbury, pp. 23–42.

L. E. Cohen and M. Felson (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review* 44:588–608.

D. R. Cressey (1953). *Other People's Money: A Study in the Social Psychology of Embezzlement*. Belmont, CA: Wadsworth.

D. J. DeLong (1998). Strikes, lockouts, labour relations. In *Protection Officer Training Manual*, eds. R. R. Minion and S. J. Davies. Woburn, MA: Butterworth-Heinemann.

F. J. Elliott (1998). Substance abuse. In *Protection Officer Training Manual*, eds. R. R. Minion and S. J. Davies. Woburn, MA: Butterworth-Heinemann.

N. H. Fishman (2000). Signs of fraud: Theft of goods and services by employees. *The CPA Journal* 70(12), Online.
C. A. Hertig (1998). Security/loss control investigations In *Protection Officer Training Manual*, eds. R. R. Minion and S. J. Davies. Woburn, MA: Butterworth-Heinemann.
R. C. Hollinger and J. P. Clark (1983). *Theft by Employees*. Lexington, MA: D.C. Heath and Company.
D. J. Horan (1997). *The Retailer's Guide to Loss Prevention and Security*. Boca Raton, FL: CRC Press.

Internal Loss

Quiz

Please refer to course text chapters and class notes.

1. _____ error technique is used to determine if an error will be detected at a point-of-sale terminal.
2. _____ analysis can be used to analyze vulnerability, better understand crime events as well as accident events. It operates by dividing _____ into _____ separate segments for analysis. It can also be used for investigating uses of force by police or security officers.
3. _____ gives the designation of "Certified Fraud Examiner."
4. "Rolling-ball effect" is a term used to describe cultural/group behavior in an internal theft/loss scenario. It is a synonym for " _____ windows" which describes a breakdown in order, vandalism, etc., in an external environment.
5. The hiring of _____ staff can raise the potential for internal theft. In some cases, these staff are hired by a contract firm.
6. _____ about employee theft should be both verbal and written.
7. Donald R. _____ authored the seminal study on embezzlement.
8. _____ audits are used to determine if procedures are being followed; _____ audits are used to uncover fiscal irregularities.
9. What types of crimes are common in each of the following cultures:
   "Work hard/play hard" _____
   "Process" _____
   "Bet your company" _____
   "Tough guy" _____
10. List the steps to be followed in a progressive discipline system moving from the least severe to most severe sanctions available to employers. _____

UNIT

VII

Physical Security and Technology

This page intentionally left blank

1 Security Systems Design and Evaluation

Mary Lynn Garcia

Introduction

The design of an effective physical protection system (PPS) requires a methodical approach in which the designer weighs the objectives of the PPS against available resources and then evaluates the proposed design. Without this kind of careful assessment, the PPS might waste valuable resources on unnecessary protection or, worse yet, fail to provide adequate protection at critical points of the facility. For example, it would probably be unwise to protect a facility's employee cafeteria with the same level of protection as the facility's central computing area. Similarly, maximum security at a facility's main entrance would be wasted if entry was also possible through an unguarded cafeteria loading dock. Each facility is unique, even if performing generally the same activities, so this systematic approach allows flexibility in the application of security tools to address local conditions.

The process of designing and analyzing a PPS is described in the remainder of this chapter. The methodology presented here is the same as that used by the United States Department of Energy (DOE) when designing PPS for critical nuclear assets.[1] This approach and supporting tools were developed and validated over the past 25 years through DOE-funded research and development totaling over $200 million. While other industrial and governmental assets may not require the highest levels of security used at nuclear weapon sites, the approach is the same whether protecting a manufacturing facility, an oil refinery, or a retail store. The foundation of this approach is the design of a performance-based system. Performance measures (i.e., validated numeric characteristics) for various system components such as sensors, video, or response time allows the use of models to predict system performance versus the identified threat. This effectiveness measure can then be used to provide the business rationale for investing in the system or upgrade, based on a measurable increase in system performance. A cost–benefit analysis can then be supported by looking at system improvement compared to costs. Before describing this process in more detail, it is necessary to differentiate between *safety* and *security*.

For the purposes of this chapter, safety is meant to represent the operation of systems in abnormal environments, such as flood, fire, earthquake, or electrical faults. Security, on the other hand, refers to systems used to prevent or detect an attack by a malevolent human adversary. There are some overlaps between the two; for example, the response to a fire may be the same whether the fire is the result of an electrical short or a terrorist bomb. It is useful, however, to recognize that a fire has no powers of reasoning, while adversaries do. A fire burns as long as there is fuel and oxygen; if these elements are removed, the fire goes out. An attack by a malevolent human adversary, on the other hand, requires that we recognize the capability of the human adversary to adapt and thus eventually defeat the security system.

[1] James E. Chapek and Paul Ebel, "Systematic Design of Physical Protection Systems," presented at 12th Annual American Defense Preparedness Association Symposium on Security Technology, June 17–20, 1996, Williamsburg, VA.

In the event of a safety critical event, such as a fire, security personnel should have a defined role in assisting, without compromising the security readiness of a facility. In this regard, security personnel should not be overloaded with safety-related tasks, as this may increase exposure of the facility to a security event during an emergency condition, particularly if the adversary creates this event as a diversion or takes advantage of the opportunity. In addition, security personnel may not possess the specific knowledge or training to respond to safety events. For example, in case of a fire, security personnel should not be expected to shutdown power or equipment. This task is better left to those familiar with the operation and shutdown of equipment, power, or production lines. Procedures describing the role of security personnel in these events should be developed, understood, and practiced in order to ensure adequate levels of protection and safety.

The design of an effective PPS includes the determination of the PPS objectives, the initial design or characterization of a PPS, the evaluation of the design, and, probably, a redesign or refinement of the system. To develop the objectives, the designer must begin by gathering information about facility operations and conditions, such as a comprehensive description of the facility, operating states, and the physical protection requirements. The designer then needs to define the threat. This involves considering factors about potential adversaries: class of adversary, adversary's capabilities, and range of adversary's tactics. Next, the designer should identify targets. Targets may be physical assets, electronic data, people, or anything that could impact business operations. The designer now knows the objectives of the PPS, that is, "what to protect against whom." The next step is to design the new system or characterize the existing system. If designing a new system, the designer must determine how best to integrate people, procedures, and equipment to meet the objectives of the system. Once a PPS is designed or characterized, it must be analyzed and evaluated to ensure it meets the physical protection objectives. Evaluation must allow for features working together to ensure protection rather than regarding each feature separately. Because of the complexity of protection systems, an evaluation usually requires modeling techniques. If any vulnerabilities are found, the initial system must be redesigned to correct the vulnerabilities and a reevaluation conducted.

PPS Design and Evaluation Process Objectives

A graphical representation of the PPS methodology is shown in Figure 1.1. As stated previously, the first step in the process is to determine the objectives of the protection system. To formulate these objectives, the designer must (1) characterize (understand) the facility operations and conditions, (2) define the threat, and (3) identify the targets.

Facility operations and conditions characterization requires developing a thorough description of the facility itself (the location of the site boundary, building location, building interior floor plans, access points). A description of the processes within the facility is also required, as well as identification of any existing physical protection features. This information can be obtained from several sources, including facility design blueprints, process descriptions, safety analysis reports, and environmental impact statements. In addition to acquisition and review of such documentation, a tour of the site under consideration and interviews with facility personnel are necessary. This provides an understanding of the physical protection requirements for the facility as well as an appreciation for the operational and safety constraints that must be considered. Many checklists exist to aid in this process[2–6]; however, since each facility

---

[2] Robert L. Barnard (1988). *Intrusion Detection Systems*. Stoneham, MA: Butterworth Publishers, pp. 7–15.

[3] Howard W. Timm and Kenneth E. Christian (1991). *Introduction to Private Security*. Pacific Grove, CA: Brooks-Cole Publishing, pp. 124–128.

[4] Harvey Burstein (1994). *Introduction to Security*. Englewood Cliffs, NJ: Prentice Hall, pp. 217–230.

[5] Karen M. Hess and Henry M. Wrobleski (1996). *Introduction to Private Security*. St. Paul, MN: West Publishing, pp. 723–732.

[6] Lawrence J. Fennelly (1996). *Handbook of Loss Prevention and Crime Prevention*. Newton, MA: Butterworth-Heinemann, pp. 33–54.

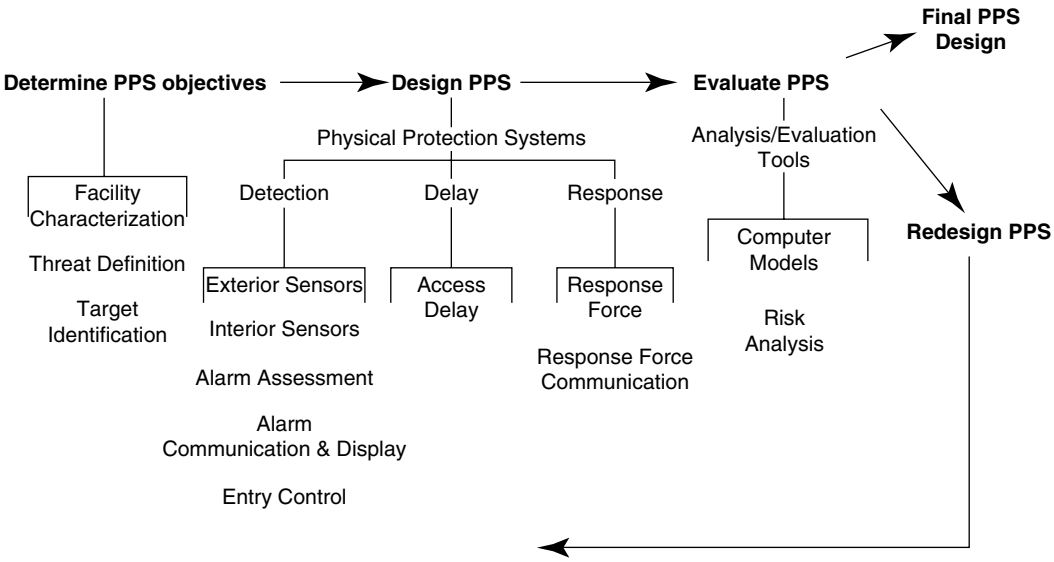


FIGURE 1.1 Design and Evaluation Process for Physical Protection Systems.

is unique, overreliance on checklists should be avoided. Compromises must usually be made on all sides so that operation can continue in a safe and efficient environment while physical protection is maintained. Additional considerations also include an understanding of liability and any legal or regulatory requirements that must be followed.

Next, a threat definition for the facility must be made. Information must be collected to answer three questions about the adversary:

1. What class of adversary is to be considered?
2. What is the range of the adversary's tactics?
3. What are the adversary's capabilities?

Adversaries can be separated into three classes: outsiders, insiders, and outsiders in collusion with insiders. For each class of adversary, the full range of tactics (deceit, force, stealth, or any combination of these) should be considered. Deceit is the attempted defeat of a security system by using false authorization and identification; force is the overt, forcible attempt to overcome a security system; and stealth is the attempt to defeat the detection system and enter the facility covertly.

Important capabilities for the adversary include knowledge of the PPS, level of motivation, any skills that would be useful in the attack, the speed with which the attack is carried out, and ability to carry tools and weapons. Since it is not generally possible to test and evaluate all possible capabilities of an unknown adversary, the designer and the analyst must make assumptions. These assumptions can be based on published information about human performance and the tested vulnerabilities of physical protection elements. Other factors to be considered are the emergency response capabilities and any critical asset tracking and inventory conditions. Consideration of the threat early in the process ensures that an appropriate and effective system is designed and implemented. If the primary threat is a vandal, we would not want to implement an expensive PPS that is more suited to a highly trained terrorist. Similarly, if the threat is a motivated criminal, we would implement a system that is capable of detecting and stopping this intruder. For any given facility there may be several threats, such as a criminal outsider, a disgruntled employee, competitors, or some combination of the above, so the PPS must be designed to protect against all of these threats. This process can be facilitated by choosing the highest credible threat, designing the system to meet this threat, and then testing to verify the system performance against the lower threats.

Finally, target identification should be performed for the facility. Targets may include critical assets or information, people, or critical areas and processes. A thorough review of the facility and its assets should be conducted. Such questions as "What asset will cost the most to replace if stolen?" or "What losses will be incurred in the event of sabotage of this equipment?" will help identify the assets or equipment that are most vulnerable or that create an unacceptable consequence.

Given the information obtained through facility characterization, threat definition, and target identification, the designer can determine the protection objectives of the PPS. An example of a protection objective might be to "interrupt a criminal adversary with hand tools and a vehicle before he or she can remove finished CPUs from the shipping dock."

The next step in the process, if designing a new PPS, is to determine how best to combine such elements as fences, barriers, sensors, procedures, communication devices, and security personnel into a PPS that can achieve the protection objectives. The resulting PPS design should meet these objectives within the operational, safety, legal, and economic constraints of the facility. The primary functions of a PPS are detection of an adversary, delay of that adversary, and response by security personnel (guard force).

Certain guidelines should be observed during the PPS design. A PPS system is generally better if detection is as far from the target as possible and delays are near the target. In addition, there is close association between detection (exterior or interior) and assessment. The designer should be aware that detection without assessment is not detection. Another close association is the relationship between response and response force communications. A response force cannot respond unless it receives a communication call for a response. These and many other particular features of PPS components help to ensure that the designer takes advantage of the strengths of each piece of equipment and uses equipment in combinations that complement each other and protect any weaknesses.

Analysis and evaluation of the PPS design begins with a review and thorough understanding of the protection objectives the designed system must meet. This can be done simply by checking for required features of a PPS, such as intrusion detection, entry control, access delay, response communications, and a protective force. However, a PPS design based on required features cannot be expected to lead to a high-performance system unless these features, when used together, are sufficient to ensure adequate levels of protection. More sophisticated analysis and evaluation techniques can be used to estimate the minimum performance levels achieved by a PPS.

An existing PPS at an operational facility cannot normally be fully tested as a system. This sort of test would be highly disruptive to the operation of the facility and could impact production schedules, as well as security effectiveness (i.e., create a vulnerability). Since direct system tests are not practical, evaluation techniques are based on performance tests of component subsystems. Component performance estimates are combined into system performance estimates by the application of system modeling techniques.

The end result of this phase of the design and analysis process is a system vulnerability assessment. Analysis of the PPS design will either find that the design effectively achieved the protection objectives or identify weaknesses. If the protection objectives are achieved, the design and analysis process is completed. However, the PPS should be analyzed periodically to ensure that the original protection objectives remain valid and that the protection system continues to meet them.

If the PPS is found ineffective, vulnerabilities in the system can be identified. The next step in the design and analysis cycle is to redesign or upgrade the initial protection system design to correct the noted vulnerabilities. It is possible that the PPS objectives also need to be reevaluated. An analysis of the redesigned system is performed. This cycle continues until the results indicate that the PPS meets the protection objectives.

PPS Design

A system may be defined as a collection of components or elements designed to achieve an objective according to a plan. The designer of any system must have the system's ultimate objective in mind. The ultimate objective of a PPS is to prevent the accomplishment of

unauthorized overt or covert actions. Typical objectives are to prevent sabotage of critical equipment, theft of assets, or information from within the facility and protection of people (executive protection or workplace violence). A PPS must accomplish its objectives by either deterrence or a combination of detection, delay, and response. Listed below are the component subsystems that provide the tools to perform these functions.

Detection
- Exterior/Interior Intrusion Sensors
- Alarm Assessment
- Alarm Communication and Display
- Entry Control Systems

Delay
- Access Delay

Response
- Response Force
- Response Force Communications

The system functions of detection and delay can be accomplished by the use of either hardware and/or guards. Response is handled by the guards. There is always a balance between the use of hardware and the use of guards. In different conditions and applications, one is often the preferable choice. The key to a successful system is the integration of people, procedures, and equipment into a system that protects the targets from the threats.

Detection, delay, and response are all required functions of an effective PPS. These functions must be performed in order and within a length of time that is less than the time required for the adversary to complete the task. A well-designed system provides protection-in-depth, minimizes the consequences of component failures, and exhibits balanced protection. In addition, a design process based on performance criteria rather than feature criteria will select elements and procedures according to the contribution they make to overall system performance. Performance criteria are also measurable, and so they can help in the analysis of the designed system.

PPS Functions

Theft and sabotage of the facility may be prevented in two ways: by deterring the adversary or by defeating the adversary. Deterrence occurs by implementing a PPS that is seen by potential adversaries as too difficult to defeat; it makes the facility an unattractive target. Examples of deterrents are the presence of security guards in parking lots, adequate lighting at night, posting of signs, and the use of barriers such as bars on windows. The problem with deterrence is that it is impossible to measure. It would be a mistake to assume that because a system has not been challenged by an adversary, the effectiveness of the system has been proven. The deterrence function of a PPS is difficult to measure and reliance on successful deterrence can be risky; thus it is considered a secondary function and will not be discussed further in this chapter.

Defeating the adversary refers to the actions taken by the response force to prevent an adversary from accomplishing his or her goal once he or she actually begins a malevolent action against a facility. There are several functions that the PPS must perform. The primary PPS functions are detection, delay, and response. It is essential to consider the system functions in detail, since a thorough understanding of the definitions of these functions and the measure of effectiveness of each is required to evaluate the system. It is important to note that detection must be accomplished for delay to be effective. Recall, the system goal is to protect assets from theft or sabotage by a malevolent adversary. For a system to be effective at this objective, we must start by knowing that we are under attack (detection), then keep the adversary away from the targets (delay), thus allowing the response force time to interrupt or stop the adversary (response).

The PPS must perform the functions of detection, delay, and response. These functions must be performed in a period of time that is less than the time required for the adversary

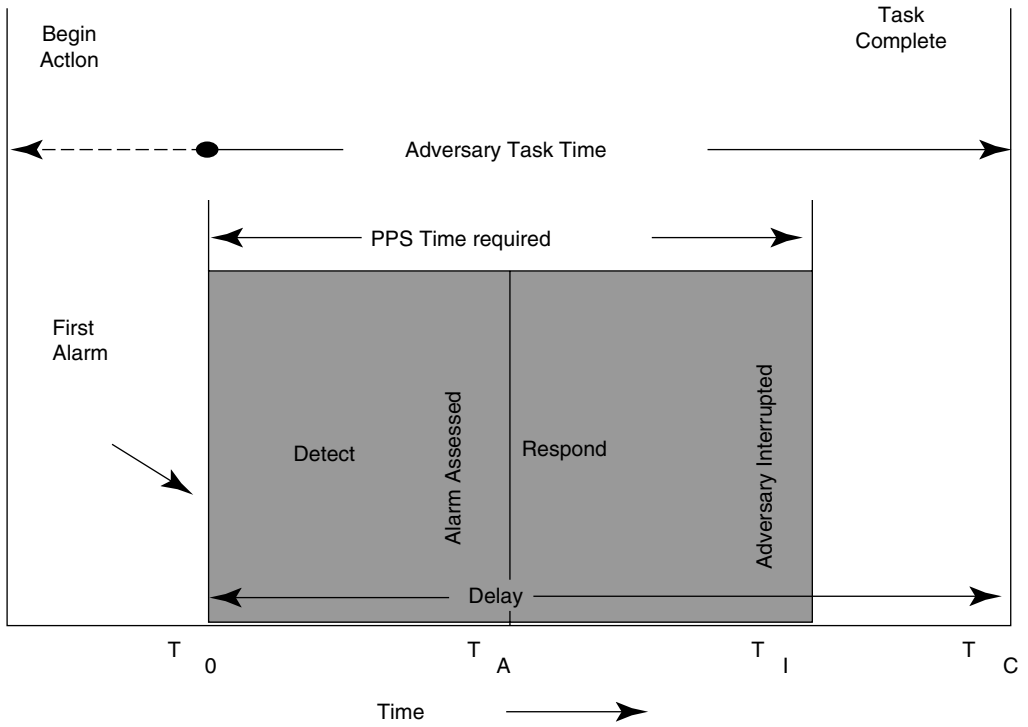


FIGURE 1.2 Adversary Task Time versus PPS Time Requirements.

to complete his or her tasks. Figure 1.2 shows the relationships between adversary task time and the time required for the PPS to do its job. The total time required for the adversary to accomplish his or her goal has been labeled Adversary Task Time. It is dependent on the delay provided by the PPS. The adversary may begin the task at some time before the first alarm sounds, labeled on the diagram as T_0. The adversary task time is shown by a dotted line before this point because delay is not effective before detection. After that alarm, the alarm information must be reported and assessed to determine if the alarm is valid. The time at which the alarm is assessed to be valid is labeled T_A, and at this time the location of the alarm must be communicated to the members of the response force. Further time is then required for the response force to respond in adequate numbers and with adequate equipment to interrupt and neutralize the adversary actions. The time at which the response force interrupts adversary actions is labeled T_I, and adversary task completion time is labeled T_C. Clearly, in order for the PPS to accomplish its objective, T_I, must occur before T_C. It is equally clear that detection (the first alarm) should occur as early as possible and T_0 (as well as T_A and T_I) should be as far to the left on the time axis as possible.

Detection

Detection is the discovery of an adversary action. It includes sensing of covert or overt actions. In order to discover an adversary action, the following events need to occur:

1. A sensor reacts to an abnormal occurrence and initiates an alarm.
2. The information from the sensor and assessment subsystems is reported and displayed.
3. A person assesses information and judges the alarm to be valid or invalid. If assessed to be a nuisance alarm, a detection has not occurred. Therefore, detection without assessment is not considered detection. Assessment is the process of determining whether the source of the alarm is due to an attack or a nuisance alarm.

Included in the detection function of physical protection is entry control. Entry control means allowing entry to authorized personnel and detecting the attempted entry of unauthorized personnel and material. The measures of effectiveness of entry control are throughput, impostor pass rate, and false rejection rate. Throughput is defined as the number of authorized personnel allowed access per unit time, assuming that all personnel who attempt entry are authorized for entrance. Impostor pass rate is the rate at which false identities or credentials are allowed entry.

The measures of effectiveness of the detection function are the probability of sensing adversary action and the time required for reporting and assessing the alarm. A sensor activates at time T_0, then at a later time a person receives information from the sensor and assessment subsystems. If the time delay between when the sensor activates and when the alarm is assessed is short, the probability of detection, P_D, will be close to the probability that the sensor will sense the unauthorized action, P_S. The probability of detection decreases as the time before assessment increases.

Detection can also be accomplished by the protective force or personnel. Guards at fixed posts or on patrol may serve a vital role in sensing an intrusion. An effective assessment system provides two types of information associated with detection: information about whether the alarm is a valid alarm or a nuisance alarm and details about the cause of the alarm—what, who, where, and how many. However, even when assisted by a video assessment system, humans do not make good detectors. Studies have shown that brief instances of movement are missed by 48% of human observers using video monitors.[7]

Delay

Delay is the second function of a PPS. It is the slowing down of adversary progress. Delay can be accomplished by barriers, locks, and activated delays. The protective force personnel can be considered elements of delay if they are in fixed and well-protected positions. The measure of delay effectiveness is the time required by the adversary (after detection) to bypass each delay element. Although the adversary may be delayed prior to detection, this delay is of no value to the effectiveness of the PPS since it does not provide additional time to respond to the adversary. Delay before detection is primarily a deterrent.

Response

The response function consists of the actions taken by the protective force to prevent adversary success. Response, as it is used here, consists of interruption. Interruption is defined as a sufficient number of response force personnel arriving at the appropriate location to stop the adversary's progress. It includes the communication of accurate information about adversary actions to the protection force and the deployment of the response force. The measure of response effectiveness is the time between receipt of a communication of adversary action and the interruption of the adversary action.

The effectiveness measures for response communication are the probability of accurate communication and the time required to communicate. The time after information is initially transmitted may vary considerably depending on the method of communication. After the initial period, the probability of valid communication begins to increase rapidly. As shown in Figure 1.3, with each repeat, the probability of correct and current data being communicated is increased. There is some delay in establishing accurate communication due to human behavior. On the first attempt to communicate, the operator is alerted that there is a call. Then a request for a second transmission is made, and finally, the operator understands the call and starts to ask for additional details.

---

[7] A. H. Tickner, D. C. V. Simmonds, *et al.* (1972). "Monitoring 16 television screens showing little movement," *Ergonomics* 15(3):279–292.

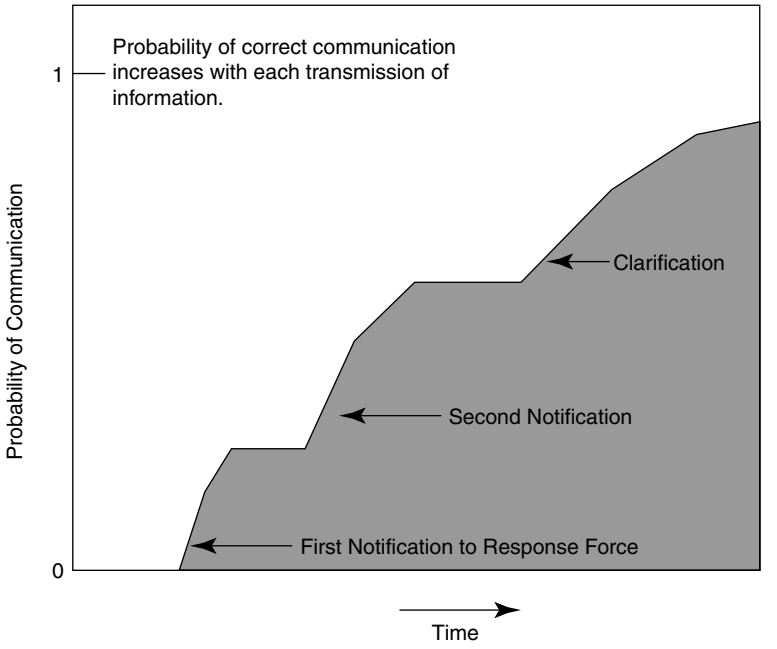


FIGURE 1.3 Variation of Probability of Valid Communication with Time.

Deployment describes the actions of the protective force from the time communication is received until the time the force is in position to interrupt the adversary. The effectiveness measure of this function is the probability of deployment to the adversary location and the time required to deploy the response force.

The effectiveness of the PPS functions of detection, delay, and response and their relationships have already been discussed. In addition, all of the hardware elements of the system must be installed, maintained, and operated properly. The procedures of the PPS must be compatible with the facility procedures. Security, safety, and operational objectives must be accomplished at all times. A PPS that has been well engineered will include the following characteristics:

- protection-in-depth;
- minimum consequence of component failure; and
- balanced protection.

Protection-in-depth means that to accomplish the goal, an adversary should be required to avoid or defeat a number of protective devices in sequence. For example, an adversary might have to defeat one sensor and penetrate two separate barriers before gaining entry to a process control room or a filing cabinet in the project costing area. The actions and times required to penetrate each of these layers may not necessarily be equal, and the effectiveness of each may be quite different, but each will require a separate and distinct act by the adversary as he or she moves along his or her path. The effect produced on the adversary by a system that provides protection-in-depth will be

- to increase uncertainty about the system;
- to require more extensive preparations prior to attacking the system; and
- to create additional steps where the adversary may fail or abort the mission.

It is unlikely that a complex system that does not experience some component failure during its lifetime will ever be developed and operated. Causes of component failure in a PPS are numerous and can range from environmental factors (which may be expected) to adversary actions beyond the scope of the threat used in the system design. Although it is important to know the cause of component failure to restore the system to normal operation, it is more important that contingency plans are provided so that the system can continue to operate. Requiring portions of these contingency plans to be carried out automatically (so that redundant equipment automatically takes over the function of disabled equipment) may be highly desirable in some cases. Some component failures may require aid from sources outside of the facility in order to minimize the impact of the failure. One example of this is the use of local law enforcement to supplement airport security personnel at times of higher alert status.

Balanced protection implies that no matter how an adversary attempts to accomplish his or her goal, he or she will encounter effective elements of the PPS. Consider, for example, the barrier surface that surrounds a room. This surface may consist of

- walls, floors, and ceilings of several types;
- doors of several types; equipment hatches in floors and ceilings; and
- heating, ventilating, and air conditioning openings with various types of grilles.

For a completely balanced system, the minimum time to penetrate each of these barriers would be equal, and the minimum probability of detecting penetration of each of these barriers should be equal. However, complete balance is probably not possible or desirable. Certain elements, such as walls, may be extremely resistant to penetration, not because of physical protection requirements but because of structural or safety requirements. Door, hatch, and grille delays may be considerably less than wall delays and still be adequate. There is no advantage in overdesigning by installing a costly door that would take several minutes to penetrate with explosives, if the wall were corrugated asbestos that could be penetrated in a few seconds with hand tools.

Finally, features designed to protect against one form of threat should not be eliminated because they overprotect against another threat. The objective should be to provide adequate protection against all threats on all possible paths and to maintain a balance with other considerations such as cost, safety, or structural integrity.

Design Criteria

Any design process must have criteria against which elements of the design will be measured. A design process based on performance criteria will select elements and procedures according to the contribution they make to overall system performance. The effectiveness measure will be overall system performance.

A feature criteria approach selects elements or procedures to satisfy requirements that certain items be present. The effectiveness measure is the presence of those features. The use of a feature criteria approach in regulations or requirements that apply to PPS should generally be avoided or handled with extreme care. Unless such care is exercised, the feature criteria approach can lead to the use of a "checklist" method to determine system adequacy based on the presence or absence of required features. This is clearly not desirable, since overall system performance is of interest, rather than the mere presence or absence of system features or components. For example, a performance criterion for a perimeter detection system would be that the system be able to detect a running intruder using any attack method. A feature criterion for the same detection system might be that the system include two specific sensor types.

The conceptual design techniques presented in this chapter are based on a performance-based approach to meeting the PPS objectives. Much of the component technology material will, however, be applicable for either performance criteria or feature criteria design methods.

The performance measures for these functions are as follows:

Detection
- Probability of detection
- Time for communication and assessment
- Frequency of nuisance alarms

Delay
- Time to defeat obstacles

Response
- Probability of accurate communication to response force
- Time to communicate
- Probability of deployment to adversary location
- Time to deploy
- Response force effectiveness

Intrusion Sensors

Intrusion detection is defined as the detection of a person or vehicle attempting to gain unauthorized entry into an area that is being protected. The intrusion detection boundary is ideally a sphere enclosing the item being protected so that all intrusions, whether by surface, air, underwater, or underground, are detected. Intrusion detection systems consist of exterior and interior intrusion sensors, video alarm assessment, entry control, and alarm communication systems all working together. Exterior sensors are those used in an outdoor environment, and interior sensors are those used inside buildings. The integration of individual sensors into a sensor system must consider specific design goals, the effects of physical and environmental conditions, and the interaction of the sensor system with a balanced and integrated PPS. Topography, vegetation, wildlife, background noise, climate and weather, and soil conditions and pavement all affect the performance of exterior sensors. Interior sensor application classes include boundary penetration sensors, interior motion sensors, and proximity sensors. Various sensor technologies can be applied to achieve protection-in-depth: at the boundary, within the room, and at the object to be protected. The designer of a good interior intrusion detection system considers the operational, physical, and environmental characteristics of the facility. Also, the designer should be familiar with the sensors that are available, how the sensors interact with the intruder and the environment, and the physical principles of operation for each sensor. Detailed descriptions of various intrusion detection components and technologies have intentionally not been included in this discussion, since it is most important for the security supervisor to understand and apply the process than to be an expert on component hardware. Many technology reviews exist and serve as excellent references for specific sensor types.[8–10]

Intrusion sensor performance is described by three fundamental characteristics:

- probability of detection, P_D
- nuisance alarm rate
- vulnerability to defeat

---

[8] Neil Cumming (1992). *Security*. Newton, MA: Butterworth-Heinemann, pp. 79–171.

[9] Lawrence J. Fennelly (1996). *Handbook of Loss Prevention and Crime Prevention*, Newton, MA: Butterworth-Heinemann, pp. 268–280.

[10] Robert L. Barnard (1988). *Intrusion Detection Systems*. Stoneham, MA: Butterworth Publishers, pp. 71–217.

For the ideal sensor, the P_D of an intrusion sensor is one (1.0). That is, it has a 100% probability of detection. However, no sensor is ideal, and the P_D is always less than 1.0. Even with thousands of tests, the P_D approaches only 1. The probability of detection depends primarily on

- threat to be detected;
- sensor hardware design;
- installation conditions;
- sensitivity adjustment;
- weather conditions; and
- condition of the equipment.

All of the above conditions can vary and, thus, despite the claims of some sensor manufacturers, a specific P_D cannot be assigned to a piece or set of sensor hardware.

A nuisance alarm is any alarm that is not caused by an intrusion. In an ideal sensor system, the nuisance alarm rate would be zero. However, in the real world all sensors interact with their environment, and they cannot discriminate between intrusions and other events in their detection zone. This is why an alarm assessment system is needed: not all sensor alarms are caused by intrusions.

Usually nuisance alarms are further classified by source. Both natural and industrial environments can cause nuisance alarms. Common sources of natural noise are vegetation (trees and weeds), wildlife (animals and birds), and weather conditions (wind, rain, snow, fog, lightning). Industrial sources of noise include ground vibration, debris moved by wind, and electromagnetic interference. False alarms are those nuisance alarms generated by the equipment itself (whether by poor design, inadequate maintenance, or component failure).

An ideal sensor could not be defeated; however, all existing sensors can be defeated. The objective of the PPS designer is to make the system very difficult to defeat.

There are two general ways to defeat the system:

- Bypass—Because all intrusion sensors have a finite detection zone, any sensor can be defeated by going around its detection volume.
- Spoof—Spoofing is any technique that allows the target to pass through the sensor's normal detection zone without generating an alarm.

Integration with Assessment System

Many intrusion detection systems use a closed circuit television (CCTV) system to perform alarm assessment. For both the sensor and video systems to perform well, care must be taken to ensure that the designs of the two systems or subsystems are compatible. Assessment may take place via the use of CCTV systems or manually by people. Video assessment automatically tied to sensor activation greatly reduces the amount of time required to determine the alarm source, thereby maximizing the use of any remaining delay and increasing the chance of successful interruption of the adversary. Video assessment also allows remote evaluation of the alarm condition, which eliminates the need to constantly dispatch guards to determine the cause of the alarm, perhaps too late to make an accurate assessment. In addition, as noted previously, people make very poor detectors, so an integrated sensor and video system should only present alarms and associated video to the operator on a single monitor, and not depend on the operator observing multiple monitors or scanning of multiple cameras on one or two monitors to detect suspicious events without the aid of sensors. Studies have shown that use of multiple screens is not as effective as use of one screen and that after one hour of observation, there is significant degradation in the human operator's ability to identify significant events.[11] Presentation of *all* camera formation continuously on

[11] A. H. Tickner, D. C. V. Simmonds, *et al.* (1972). "Monitoring 16 television screens showing a great deal of movement," *Ergonomics* 16(4):381–402.

several monitors, particularly by scanning, reduces the probability of detection of an event and decreases system performance.

Additional considerations in this area include size of the zone to be assessed and location of the camera. Larger zones require the use of less equipment, while smaller zones can give better resolution. Consideration of the image to be viewed should drive this decision. For example, if it is important only to know that a person has intruded into an area, a wider or longer zone may be used. If, however, specific details of the person are required, shorter zones will be required. For video assessment systems to be effective, the area under surveillance must be adequately lit, to allow a rapid and accurate assessment.

In addition, the camera must be positioned to view the entire area being assessed (i.e., no blind spots). The sensors must be placed so that on an alarm, the camera viewing the zone will have an unobstructed view of the entire zone. To achieve maximum system effectiveness, fixed cameras, aimed at the area of interest, should be used. Use of pan-tilt-zoom (PTZ) cameras should be limited to use for secondary assessment or surveillance only, since it is unlikely that a PTZ camera will be pointing in the appropriate direction on alarm and thus may reduce the chances for an accurate and timely assessment. Technical references on the use and design of CCTV systems and components are readily available.[12,13]

Integration with Barrier Delay System

Balanced integrated PPS usually incorporate some type of barrier or access denial systems to provide delay time for video assessment of the alarm source and for the response force to respond to an intrusion. In many cases this includes some type of barrier installed at the perimeter; however, the barrier should not degrade the performance of the sensors. Perimeter barriers are usually installed on or near the innermost fence so that an intruder cannot tamper with or defeat the barrier without first passing through a detection zone. This placement is important to ensure that the response action is initiated before the delay occurs. Barriers should not distort the sensors' detection volume, cause nuisance alarms, or obscure part of the camera's view.

Response

The meaning of the phrase "response force" varies from facility to facility. A part of or all of the response force may be located on-site or off-site. The response force may include local and state police, and dedicated response teams at the facility. These response forces may be armed or unarmed. In addition, response may be broken into two major categories—immediate on-site response (i.e., timely response) and recovery. Depending on the needs and objectives of a facility, it is prudent to decide in advance which strategy will be used at the site. Different targets may require different strategies. For example, stopping an intruder about to sabotage a critical valve in a refinery may require an immediate on-site response, while recovery may be a better technique for theft of company-owned tools. For a recovery-based response, the use of videotape for after-the-fact review can be very effective and legally acceptable. It should be apparent that timely response will require better detection and delay than a response strategy that focuses on recovery of the asset. The difficulty with recovery as a strategy is that it may not matter if stolen documents or information are recovered, since the adversary may have copied the information. In a like manner, once an incident of workplace violence has occurred, the capture of the perpetrator is commendable; however, there is still the aftermath of the event to consider. This aftermath may include legal action by the victim against the facility, bad publicity for the facility, poor employee morale, and regulatory action against the facility.

Because of these variables, it is difficult to generalize about specific procedures or tasks that the response force may be expected to perform. The final result is that the response force

---

[12] Herman Kruegle (1995). *CCTV Surveillance: Video Practices and Technology*, Newton, MA: Butterworth-Heinemann, pp. 65–126.

[13] Robert L. Barnard (1988). *Intrusion Detection Systems*. Stoneham, MA: Butterworth Publishers, pp. 221–349.

must prevent the adversaries from accomplishing their objective. Specific task assignments to accomplish this function will be reflected in variations of qualification standards, training requirements, and performance standards as measured by realistic tests. In this discussion, the PPS function of response has been divided into three parts: contingency planning, communication, and interruption.

Contingency planning is an important part of a facility's ability to successfully resolve an incident. Prior planning will help a facility manger identify potential targets, how to respond to different threats, how the facility will interact with outside agencies, as well as what level of force facility personnel will use in various situations. Well-documented procedures should be developed in advance as a major part of contingency planning.

Tactical planning should be part of contingency planning in general. Procedures and plans for guard actions in the event of a true alarm should be well established. The chain of command and the succession of command in case of emergency should be well known. Plans must be made to ensure that members of the response force possess or have rapid access to the proper equipment consistent with the defined threat. Tactical plans must contain specific details for the response force to deploy successfully. Response strategies (contain, deny, assault) must be well planned and practiced.

The role of the response force should also be factored into the facility contingency plan. A response force whose key role is the containment of adversaries until additional help arrives will deploy differently than a response force capable of recovery operations. It is likely that there will be two sets of guards at a facility—one group checking credentials, patrolling, and serving the deterrence/delay role and another, more highly skilled group with primary responsibility for response.

A critical part of the design and analysis process of a PPS is the identification of potential targets. Supervisors can then evaluate the likely routes an adversary may use to approach the facility boundaries, buildings, and rooms, as well as the specific target. This type of information will assist supervisors in developing detailed tactical plans to address various threats to the facility. In addition, it will be useful in determining protective force patrol routes and schedules.

Security supervisors should consider using support from outside (nonfacility) agencies as they do their contingency planning. A facility may wish to consider developing support agreements with local or state law enforcement agencies or a Mutual Aid Agreement with other sites. To facilitate this, a written support agreement with outside agencies or sites should be developed. This written agreement should detail the interaction between facility personnel and the neighboring agencies. The agreement should be developed with input from all participants affected by the agreement and approved by each organization. Issues such as the neighboring agency's role in an incident, off-site pursuit by facility response force personnel and communication should be considered. The role of the neighboring agency should be closely examined. Facility security managers may consider use of other agencies for containment and/or recovery support. These decisions will need to be based on the neighboring agency's response time, training, equipment, and availability to support the facility. Facility security managers may decide to provide their response force personnel with off-site credentials and authority to facilitate the response force's ability to operate outside of the facility's boundaries. This may be an important consideration during deployment and pursuit.

Communication will be a key factor in the interaction between facility personnel and other agencies. Since different agencies rarely operate on the same radio frequency, supervisors will need to evaluate alternate means of communication. A dedicated landline may be used for initial notification to outside agencies and preplanned routes and containment positions may help resolve on-scene communications concerns.

A critical factor that will influence the ability for a neighboring agency to successfully support a facility is joint training. Security supervisors should plan and conduct periodic training exercises with outside agencies. The scope of this training will be dictated by the supporting agency's role. If the support agency will act primarily in a containment capacity, then primary containment positions and areas of responsibility should be practiced. However, if the support agency will be conducting recovery operations, more detailed training and facility knowledge will be required.

Different threats will require responding officers to employ a wide variety of force to address any given situation. Response force personnel should have the ability to apply appropriate levels of force to stop an adversary's actions. This will include the guard's presence as a deterrent or delay, the use of intermediate force, and finally the use of deadly force. The facility should have a written policy to provide clear guidelines to the guards in the use of force.

A use-of-force policy should be based on using the minimum amount of force necessary to stop an adversary's actions. Typically the amount of force used will be dictated by the adversary's actions. For example, an unarmed adversary who is refusing to follow the instructions of a guard but does not present any other threat should be handled with less force than an adversary who is armed and posing a threat to the facility or guards. This type of policy will typically require guards to have the ability to employ intermediate force weapons such as impact (baton) or chemical (mace) weapons.

After developing a use-of-force policy, supervisors should provide response force personnel with training to ensure all personnel are well versed in the policy and the deployment of their weapons. Managers should consider semiannual or quarterly training and qualifications to ensure their personnel are capable of successful application of the facility's policy and weapons. Documentation of all training records will be useful in the event of any legal challenges or postincident reviews.

When designing a training program, it is important to consult the facility security manager and the PPS designer. The facility security manager is most familiar with the functional performance and task requirements of the response force. The facility security manager is also responsible for a separate training agenda that deals with policies, procedures, and basic training not specific to system operation (arrest powers, use of force, basic marksmanship, communications).

The PPS designer can provide input to the development of training and testing programs. The designer is most familiar with the operations and limitations of the PPS equipment and the other PPS functions (detection, delay). From the designer's point of view, the objectives of the training are to maximize the ability of the response force to use the PPS in carrying out its basic mission: protection of the assets of the facility.

In addition to tactical planning and training, it is important for the response force to practice deployment at the specific facility in exercises so they will know what to do in the event of an actual attack. Results of good practice give realistic estimates of response force times. Field exercises should be used to verify that tactical training has resulted in the desired capability and that the overall tactical plan is realistic. In order for the response force to plan and practice, the threat must be quantified either by policy or local assessment. This threat should also address whether the adversary's objective is theft, sabotage, or both.

One test of the response guards' proficiency is to determine if they can arrive quick enough after notification to interrupt the adversary. The responders require skills in addition to speed. Such skills requiring testing include marksmanship, physical fitness, use of force under stress, use of deadly and intermediate force, tactical movement, accurate response communications, target and facility familiarity, and use of PPS features to their advantage.

Some of these skills can be evaluated in simulation courses in the classroom. Others, especially the testing of the application of the skills, can take place only in the facility or something quite similar to it. The measure of proficiency being tested under engagement simulation exercises in these circumstances is the response force's ability to stop an attack. The only acceptable level of proficiency in response procedures is the prevention of damage to, or loss of, critical assets.

Communication is a vital part of the response function. The proper performance of all other system functions depends on communication. Information must be transferred through this network with both speed and reliability. Communication to the response force must contain information about adversary actions and instructions for deployment. The effectiveness measures for response communication are the probability of accurate communication and the time required to communicate to the response force. Communication includes voice and other systems that allow members of the protective and response forces to communicate with each other. The successful operation of a PPS requires a reliable response force communication network that is resistant to being used to the advantage of knowledgeable and determined adversaries.

Analysis

A PPS is a complex configuration of detection, delay, and response elements. Computerized techniques are available to analyze a PPS and evaluate its effectiveness.[14,15] Such techniques identify system deficiencies, evaluate improvements, and perform cost versus effectiveness comparisons. These techniques are appropriate for analyzing PPS at individual sites. Also, the techniques can be used for evaluating either an existing protection system or a proposed system design.

An adversary path is an ordered series of actions against a target which, if completed, results in successful theft or sabotage. Protection elements along the path detect and delay the adversary. Detection includes not only sensor activation but also alarm communication and assessment.

At a specific facility, the following factors must be considered:

1. Specific target(s) must be identified.
2. Many adversary paths to each target are possible.
3. The detection, delay, and response elements are specific to the protection system.
4. More than one threat should be considered.

Therefore, the identification and evaluation of adversary paths is usually a complex process.

A team with broad experience is necessary to ensure a complete and accurate assessment of the site is produced. The members of the team should be

- Team Leader (Security Supervisor)
- Security Systems Engineer (Detection and Communications)
- Locksmith
- Response Expert
- Access Delay Expert
- Modeling Expert
- Operations Representatives

---

[14] *Harold A. Bennett (1977). "The 'EASI' Approach to Physical Security Evaluation," *SAND Report #760500*.

[15] *L. D. Chapman and C. P. Harlan (1985). "EASI Estimate of Adversary Sequence Interruption on an IBM PC," *SAND Report #851105*.

*SAND Reports available from:
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Road
Springfield, VA 22161
Phone: 1-800-553-NTIS (6847) or
703-605-6000
Fax: 703-321-8547
TDD: 703-487-4639
Internet: http:www.ntis.gov/ordering.htm

OR

U.S. Government Printing Office
Superintendent of Documents
Federal Depository Libraries Program
Washington, D.C. 20402
Phone: 202-512-1530; 888-293-6498
Fax: 202-512-1262
Email: gpoaccess@gpo.gov
Internet: http:www.access.gpo.gov

National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Road
Springfield, VA 22161
Phone: 1-800-553-NTIS (6847) or
703-605-6000
Fax: 703-321-8547
TDD: 703-487-4639
Internet: http:www.ntis.gov/ordering.htm

OR

U.S. Government Printing Office
Superintendent of Documents
Federal Depository Libraries Program
Washington, D.C. 20402
Phone: 202-512-1530; 888-293-6498
Fax: 202-512-1262
Email: gpoaccess@gpo.gov
Internet: http:www.access.gpo.gov

The team follows the steps of the process described above, including understanding the facility, defining the threat and targets, and then designing an appropriate PPS. Once a new PPS or upgrade has been designed, a vulnerability analysis is conducted. It is a systematic way of ensuring the design meets an acceptable level of performance against adversaries identified as the design basis threat. It is important to note that this vulnerability analysis focuses on the performance of the PPS and is not a simple compliance-with-regulations check.

The goal of an adversary is to complete a path with the least likelihood of being stopped by the PPS. To achieve this goal, the adversary may attempt to minimize the time required to complete the path. This strategy involves penetrating barriers with little regard to the probability of being detected. If the adversary completes the path before guards can respond, he or she is successful. Alternatively, the adversary may attempt to minimize detection with little regard to the time required. If the adversary completes the path without being detected, he or she is successful.

One measure of PPS effectiveness is the comparison of the minimum cumulative time delay along the path compared to the guard response time. An adequate PPS provides enough delay for the guards to respond. The disadvantage of this measure of effectiveness is that no consideration of detection is involved. Delay without prior detection is not meaningful since the response force must be alerted in order to respond and interrupt the adversary. Therefore, the minimum time measure alone is not the best measure of system effectiveness.

Another measure of effectiveness is the cumulative probability of detecting the adversary before his mission is completed. An adequate protection system provides high probability of detection. For an effective system, the minimum cumulative detection along the path must be an acceptable value. The disadvantage is that no consideration of delay is involved. Detection without sufficient subsequent delay is not meaningful since the response force may have insufficient time to interrupt the adversary.

Neither delay time nor cumulative probability of detection alone is the best measure of effectiveness. A better measure of effectiveness is "timely detection." Timely detection is the *minimum cumulative probability of detecting the adversary while there is enough time remaining for the response force to interrupt the adversary*. The delay elements along the path determine the point by which the adversary must be detected. That point is where the minimum delay along the remaining portion of the path just exceeds the guard response time. The minimum cumulative probability of interruption (P_I) is the cumulative probability of detection from the start of the path up to the point determined by the time remaining for the guards to respond. This value of P_I serves as a measure of the PPS effectiveness. An example of this concept is shown at the end of the chapter.

PPS Design and the Relationship to Risk

The analysis of a PPS includes the determination of the PPS objectives, characterizing the design of the PPS, the evaluation of the design, and possibly, a redesign or refinement of the system. The process must begin by gathering information about the facility, defining the threat, and then identifying targets. Determination of whether or not the assets are attractive targets is based mainly on the ease or difficulty of acquisition and desirability of the material. The next step is to characterize the design of the PPS by determining the elements of detection, delay, and response. The PPS is then analyzed and evaluated to ensure it meets the physical protection objectives. Evaluation must allow for features working together to ensure protection rather than regarding each feature separately.

The basic premise of the methodology described in this chapter is that the design and analysis of physical protection must be done from a systems standpoint. In this way, all components of detection, delay, and response can be properly weighed according to their contribution to the PPS as a whole. At a higher level, the facility owner must balance the effectiveness of the PPS against available resources and then evaluate the proposed design. Without a methodical, defined, analytical assessment, the PPS might waste valuable resources on unnecessary protection or, worse yet, fail to provide adequate protection at critical points of the facility. Because of the complexity of protection systems, an evaluation usually requires

computer modeling techniques. If any vulnerabilities are found, the initial system must be redesigned to correct the vulnerabilities and a reevaluation conducted. Then the system overall risk should be calculated. This risk is normalized to the consequence severity if the adversary could attain the target. The facility is then able to make a judgement as to the amount of risk that exists and if this is acceptable.

There are some significant considerations of the PPS designer, the facility management, and any regulatory authority as they are charged with answering the question "How do we know if the security system is good enough?" In the previous discussion, the concept of probability of interruption of the defined adversary along the most vulnerable path in the facility was developed and identified as the best measure of PPS effectiveness. The next question is, "Given a certain P_I, is that good enough?"

The final question really is "How much risk is the facility willing to accept versus the cost of reducing that risk?" If the facility and regulators understand that there are a limited amount of resources to be applied to physical protection of everything at the facility, then each application of a portion of those resources must be carefully and analytically evaluated to ensure a balanced risk. The remainder of this chapter will briefly explain the method of risk identification and mitigation practiced by Sandia National Laboratories.

The risk equation used is:

$$R = P_A\,[1\sim(1\sim P_I)]\,C$$

where the terms are as follows:

R = *Risk to the facility (or stakeholders)* of an adversary gaining access to, or stealing, critical assets. Range is 0 to 1.0, with 0 being no risk and 1.0 being maximum risk.

P_A = *Probability of an adversary attack*. This can be difficult to determine, but generally there are records available to assist in this effort. The value of this probability is from 0 (no chance at all of an attack) to 1.0 (certainty of attack). Usually in the calculation of risk, we assume $P_A = 1.0$, which means that the risk answer is a "conditional risk." That is, the calculated risk *given* that an attack on a facility will occur.

P_I = *Probability of Interruption*. This is the probability that the defined adversary will be interrupted by the response force in time to stop the adversary from accomplishing the objectives. The principle of timely detection is used in calculating this probability from 0 (the adversary will definitely be successful) to 1.0 (the adversary will definitely be interrupted in his or her path).

C = *Consequence Value*. This is a value from 0 to 1 that relates the severity of the occurrence of the event. This is the normalizing factor that allows the conditional risk value to be compared to all other risks across the site. A consequence table of all events could be created that would cover the spectrum of loss, from highest to lowest. Therefore, by using this consequence table, the risk can be normalized over all possible events. Then the limited PPS resources can be appropriately allocated to ensure the risk is acceptable across the spectrum.

If we assume that P_A is equal to 1 (there *will* be an attack), this term drops out of the equation. If we then also assume that C is equal to 1, that is, the consequence is the highest we can imagine, this term also drops out. This leaves a conditional risk, R, that is determined solely by the effectiveness of the PPS, which can be useful in establishing the "worst case" risk—that is, an attack by the most capable adversary on the most valuable target. It is then possible to go back and use different Consequence Values to determine the risk to the enterprise for lower consequence losses. This will allow a prioritization of targets and appropriate protection. Finally, the probability of attack may also be varied, based on available data where possible, and a realistic assessment of risk can be obtained. This three-step process can help in simplifying the complexity of the risk assessment by varying only one term at a time, allowing an appreciation about the influence of each factor on the outcome.

Once the risk value is determined, the security manager can justify the expenditure of funds based on a scientific, measurable, and prioritized analysis. This information can be presented to the executive management of the corporation or facility to demonstrate how the security risk is being mitigated and how much risk exposure remains. The analysis can then form the basis for a discussion on how much security risk can be tolerated or how much to

increase or decrease the budget based on risk. This analysis can also serve to demonstrate to any regulatory agencies that a careful review of the security of the facility has been performed and that reasonable measures are in place to protect people and assets. The analysis will allow the facility to state the assumptions that were made (threat, targets, risk level), show the system design, and provide an analysis to show system effectiveness.

This process only describes the evaluated risk of the security system and its effectiveness. It should be noted that there are multiple risk areas for a facility or corporation, of which security is only one part. Other areas of risk that need to be considered within the business enterprise include financial risk management, liability risk financing, property/net income financing, employee benefits, environmental health and safety, and property engineering.[16] The facility or corporate Chief Risk Officer must still combine all of the various risks and help the corporation manage total risk. While the security department may be able to aid in mitigation of risk in other areas, the security supervisor is only one of many experts who must be depended on to ensure that the corporate enterprise manages and limits their risk exposure. Finally, this approach allows for risk control through two mechanisms. Traditional loss reduction or mitigation, which is the reduction of severity by employing methods to mitigate or minimize the impact of a loss *after* the event occurs (insurance), is very reactive. Another approach is that of loss prevention, which is the reduction of frequency by employing methods to prevent the loss from occurring. This is a more proactive risk control philosophy. Good risk programs should include a combination of risk financing (insurance) and risk control tools to treat the risk.[16]

It should be clear that the security program is one that contributes to the bottom line of the corporation, by protecting assets from malevolent human threats. The security supervisor should be capable of managing available resources to best protect corporate assets and adjusting resources as required in the face of changing threats. This is the role of the security supervisor in the corporate structure.

Summary

This chapter has covered the use of a systematic and measurable approach to the implementation of a PPS. The concept of detection, followed by delay and response, was emphasized and a brief description of the relationship of these functions was presented. Specific performance measures of various components of a PPS were described, along with how these measures are combined to support a cost–benefit analysis. The process stresses the use of integrated systems combining people, procedures, and equipment to meet the protection objectives. In support of this concept, the difference between safety and security was described to clarify the contrast between natural disasters and malevolent human attack. The role of training, particularly for the guard force, was also described.

The intent of this chapter is not to create an expert designer but to instill an appreciation of the relationship between protection objectives and the system that is implemented. This must be accomplished within the constraints of the facility, while at the same time mitigating risk to a known level. The concepts presented here are somewhat unique in the security industry as a whole but have been demonstrated to be effective in protecting critical nuclear assets for the past 25 years. Although your particular facility may not require the same level of protection, or have the same unacceptably high consequence of loss (the loss of a nuclear weapon or material could result in the death of thousands of people), the process described in these pages can still be applied to protect your targets against the appropriate threats. Ultimately, this leads to an effective system design that can be used to explain why certain security components were used, how they contribute to the system effectiveness, and how this

[16] M. Michael Zuckerman, "*Moving Towards a Holistic Approach to Risk Management Education—Teaching Business Security Management*," presented at 2nd Annual American Society of Industrial Security Education Symposium, August 13–15, 1998, New York, NY.

system mitigates total risk to the facility or corporation. This, then, is the goal of the chapter—to allow a security supervisor to discern whether or not an existing or proposed PPS has considered all pertinent information and determine if the system is effective at expected levels. Once the supervisor has collected all of this information, supported by application of rigorous criteria and validated analysis, a powerful case can be made to the executive management to justify the security department budget and role, and build recognition of the security function as a major part of the corporation's business, not just a non-value-added inconvenience.

Sample Analysis Scenario

Suppose there is a facility with a fence around the boundary, an open space, and then a few buildings with production activities taking place. A single outside criminal, with a handgun and a cutting torch, decides to break into the facility and steal an asset located in a vault in the building. The perimeter fence has a fence disturbance sensor on the part of the fence that is located at the back edge of the facility. There are two security guards on duty in the lobby of the facility, who monitor multiple PTZ cameras placed on the exterior and interior of the facility though the use of a CCTV system. There are magnetic switch contacts on all doors and Passive Infrared Sensors (PIR) in all rooms and offices in the buildings. The vault has a 4-in. thick steel door and 6-in. thick concrete walls. Inside the vault is a microwave sensor. There are no exterior guard patrols. The response time of the guards at this facility is 4 min (240 sec). Table 1.1 summarizes the adversary's steps in attacking the facility.

The detection values at steps 1 and 2 are assigned by the chance that a guard or employee may spot the attacker climbing the fence or running across the area, with no sensor technology deployed. The delay times reflect the time it takes to climb the fence and run 100 yards to the building. As the attacker enters a side door, the magnetic switch sensor has a P_D of 0.3; the door is locked and it takes 20 sec to defeat the lock. The attacker then crosses the distance from the door to the office, which has a PIR sensor. The delay time is for the attacker walking across the inner area. Next, the adversary reaches the vault and takes 5 min (300 sec) to defeat the door. The P_D of the interior microwave is 0.4. The adversary then takes the asset and starts to escape by fleeing through the same door he or she entered, crossing the open area from the side door to the rear of the property and climbing the section of the fence with the sensor, which results in a P_D of 0.3. The adversary then jumps into his or her car and escapes with the asset. The total adversary task time for this scenario is 392 sec, or approximately 6.5 min.

Computer analysis of this series of events is shown in Table 1.1. Observe that there is a 67% chance of the adversary being interrupted along this path. This is determined by going back from the target and finding the point where there is more than 240 sec of delay time left (the amount of time it will take the response force to arrive and interrupt the adversary). This indicates that if the adversary is not detected by the time he or she reaches the vault door (the first point where over 240 sec of delay remains), there will not be enough time to stop

Table 1.1 Adversary Attack Route, Initial System

Action	Probability of Detection	Delay Time (sec)
1. Climb side fence	0.1	5
2. Run to building	0.1	15
3. Open door	0.3	20
4. Move to asset	0.5	30
5. Remove asset	0.4	300
6. Exit building through outer door	0.1	5
7. Cross open area to back fence	0.3	10
8. Leave area by car	0.1	7

Table 1.2 Adversary Attack Route, Upgraded System

Action	Probability of Detection	Delay Time (sec)
1. Climb side fence	0.9	5
2. Run to building	0.1	15
3. Open door	0.3	20
4. Move to asset	0.5	30
5. Remove asset	0.4	300
6. Exit building through outer door	0.1	5
7. Cross open area to back fence	0.3	10
8. Leave area by car	0.1	7

him or her. The 0.67 represents the cumulative probability of detecting the adversary by the time he or she reaches the vault door, which is influenced by the low probability of detection up to the building. Since detection must occur *before* he or she reaches the vault door for the response force to be successful, the system does not get the benefit of the lengthy delay at the vault door, which favors the adversary. The facility security manager decides that this is not good enough, since loss of this asset would be a high consequence. She decides to add a fence sensor around the remaining three sides of the perimeter to see if this will help. She installs a different kind of fence sensor on the fence and improves the P_D to 0.9. The new value is reflected in Table 1.2.

Using this new P_D value in the model gives the result shown in Table 1.2. The probability of interruption has now improved to 93%, due to the addition of improved early detection. Now, the chances of success are much higher, since there is a much higher chance that the intruder will be detected when climbing the fence. Now, *all* of the delay time will be credited since the response force personnel know they are under attack and have ample time to respond and stop the attack.

This is a simple example, for one path, that shows the usefulness of the systematic approach to security system design and analysis of the system to predict effectiveness.

Quiz

1. Which is NOT an example of a threat tactic?
   a) Stealth
   b) Force
   c) Deceit
   d) Timely detection

2. Which of the following would cause a false alarm for an intrusion detection system?
   a) Rabbit
   b) Wind
   c) Blowing trash
   d) Component failure

3. Deterrence contributes a measurable amount to an effective physical protection system. ☐ T ☐ F

4. The probability of detection for a sensor depends primarily on
   a) Threat to be detected
   b) Sensor hardware design
   c) Installation conditions
   d) All of the above

5. In a physical security system, which is NOT a threat scenario?
   a) Theft
   b) Sabotage
   c) Kidnapping
   d) Earthquake

6. Which of the following is a performance measure for delay barriers?
   a) Location of barrier
   b) Size of barrier
   c) Time to defeat barrier
   d) Type of barrier

7. Which of the following is a performance measure for a sensor?
   a) Probability of detection
   b) Placement in the facility
   c) Technology class
   d) Detection volume

8. Detection is not complete until there has been assessment of the alarm.
   ☐ T ☐ F

9. Which of the following is NOT a performance measure for a sensor?
   a) Probability of detection
   b) Sensor application
   c) Nuisance alarm rate
   d) Vulnerability to defeat

10. Which information is NOT required to define a threat?
    a) Class of adversary—insider, outsiders, outsiders in collusion with insiders
    b) Adversary tactics—deceit, force, stealth, or a combination
    c) Adversary capabilities—knowledge, motivation, skills, tools, weapons
    d) Security System—intrusion detection system

This page intentionally left blank

2 Statistical Analysis

Whitney D. Gunter and Patricia A. O'Donoghue

Statistical analysis ultimately boils down to numerical results: the methods and processes used in obtaining them and the methods and means for estimating their reliability. You do not have to be a mathematical wizard or speak only in theorem(s); even the average person has confidence in the conclusion stated in numerical language and supported by numerical facts.

Simply put, there are three steps involved in the management of a statistical problem that can be summarized as follows:

1. The collection of data
2. The organization of data
3. The analysis of data

In order to grasp the meaning of a vast amount of numerical data, you must reduce its bulk. The process of abstracting the significant facts contained in the data and making clear and concise statements about the derived results constitutes a statistical analysis. Common sense and experience are key elements in the analysis phase of information gathering. Its purpose is to give a summarized and comprehensible numerical description of large amounts of information.

The Collection of Data

Why does a security supervisor need to learn about the collection of data or research methods? The reasons are quite simple: wouldn't it be an asset to any organization if managers could sense, spot, and deal with problems before they become serious? Knowing about research and problem-solving processes assists managers to identify problems and find out more about the situation.

Staffing Exercise

For example, consider a problem that all managers face at one time or another: the staffing of the work force. As a manager faced with this problem, you will need to collect some data. Here are some things to consider, statistically speaking. First and foremost, what is the total number of individuals that you will need to effectively run your day-to-day operation? Now let's say that 70% are considered "old" employees; that is, they have worked in your security department for more than a year. The other 30% are "new" employees with the following attrition record:

–Within the first four months of their employment, 50% leave.
–Within the second four months, 20% leave.
–Within the next four months, 10% leave.

In conclusion, only 20% make it through the first year: they become "old" employees. Among the old employees, the attrition rate is 30% a year (or 10% every four months). With these rates in mind, how should you approach the problem of determining a hiring rate that will:

1. Maintain a stable work force?
2. Reduce the work force by any given percentage rate annually? or
3. Increase the work force by any given percentage rate annually?

Once organized and analyzed, this research and data can be a useful decision-making tool rather than a mass of incomprehensible statistical information. In addition, being knowledgeable about research and research methods helps professional managers to (1) identify and solve small problems in the work setting, (2) know how to discriminate good research from bad research, (3) appreciate and constantly remember the multiple influences of factors impinging on a situation, and (4) take calculated risks in decision making, knowing fully well the probabilities attached to the different outcomes.

The Organization of Data

When a mass of data has been assembled, it is necessary to classify the material in some compact and orderly form before it can be effectively analyzed. This procedure merely takes the "ungrouped" original information and "groups" or places the information into a specific category to be utilized during periods where the information is tested for accuracy. You want to be able to work easily with the information, and organizing it into categories helps you do that.

Take, for example, the affinity diagram used in many quality initiatives. Use the affinity diagram when you want to:

1. Quickly organize diverse data and perspectives.
2. Engage everyone in the brainstorming process.
3. Surface different perspectives.
4. Promote a common understanding.

Let's consider a real life example of how to organize data. For the manager of a security force charged with maintaining some type of access control into a facility, the waiting lines and waiting-line behavior of customers is a never-ending concern. Waiting in lines (generally referred to as queues) occurs when some employees or customers wait for service and access into a facility. On the average, it is possible to be a member of at least three queues on any given day.

Hurry Up and Wait Exercise

From a manager's point of view, here are some of your considerations in trying to solve this problem of waiting in queue. The manager must try to hit a happy medium where waiting lines are short enough to minimize customer complaints keeping in mind it is clearly not practical to provide such extensive service so that no waiting line or queue can develop. In effect, managers balance the increased cost against the customer complaints (which increases as the average length of the wait increases). Data on time spent waiting in line can be organized and broken down into two categories, (1) the number of arrivals during a certain period of time and (2) the time lost by personnel waiting for services (see Chart #1). More categories can be constructed to include the sheer numbers of persons waiting in line. This information may be used to determine if another service person should be assigned to the desk during a specific time of day, say between 7:00 and 9:00 o'clock in the morning when the line is the longest.

Time analysis: 231 min or an average waiting time per arrival of 231/31 = 7.45 min.

As the chart illustrates, it is not only good customer service to provide two access control individuals at the desk, but also more importantly, it is cost effective. The Chief Financial Officer (CFO) would love to hear how you saved the company's money and utilized your personnel effectively with this one example.

Chart #1

No. of period (hours)	No. of arrivals	Service time (min)
1	0	7,7
2	2	
3	0	
4	2	10, 10
5	1	5
6	0	
7	4	6, 7, 9, 12
8	7	3, 4, 6, 7, 9, 10, 15
9	5	4, 5, 5, 7, 10
10	0	
11	0	
12	2	4, 4
13	0	
14	0	
15	0	
16	1	10
17	0	
18	4	5, 5, 7, 10
19	1	8
20	1	10
21	0	
22	0	
23	0	
24	1	10
Total	31	231

Analysis of Data

Since statistics has to do primarily with obscured measurements, which are admittedly approximations, and with processes that are also approximate, it is obvious that any numerical result obtained from them will be an approximation.

Decision Making

If it would have been possible to predict the future with complete certainty, the structure of managerial decision would be radically different from what it is. There would be no excess production, no clearance sales, and no speculation in the stock market.

As we do not live in a world of complete certainty, we usually try to make decisions by using the probability theory. Usually, managers will have some knowledge about the possible outcomes in a decision situation; by collecting and organizing information, as we've spoken about earlier, and considering it systematically, managers often will reach a sounder decision than if they try and guess.

The concept of probability is a part of our everyday lives, both personal and professional. When they predict rain, we change our plans from outdoor activities to indoor ones. Managers who manage inventories go through a series of decision-making situations similar

to when we change our original plans of having fun from outside to inside. Both these decision makers benefit from their own assessment of the chances that certain things will happen.

Probability is the chance that something will happen. In probability theory, an event is one or more of the possible outcomes of doing something. For example, let's examine the classic coin-toss event. We all know if we toss a coin getting a tail would be an event and getting a head would be another event. This activity of tossing the coin in probability theory is called an experiment.

Most managers, like yourself, are much less excited about coin tossing than they are in the answers to questions like, "Did we order enough blazers?" or "What are the chances that our uniforms will arrive in time for the annual meeting?" or "Will the transportation strike affect our shipment of shirts?"

When conducting experiments in probability, there are two terms that you should be familiar with: *mutually exclusive* and *collectively exhaustive* events.

Events are mutually exclusive if one and only one of them takes place at a time. Consider again the example of the coin toss. We have two possible outcomes, heads or tails. On any single toss, either heads or tails may turn up, but not both. Accordingly, the events heads and tails on a single toss are said to be mutually exclusive. The question you should ask yourself, in determining whether the events are mutually exclusive, is can two or more of these events occur at one time? If the answer is yes, the events are not mutually exclusive.

When you make a list of possible events that can result from an experiment and this list includes every possible outcome, you have a collectively exhaustive list. In the coin toss example, the list "heads and tails" is collectively exhaustive—unless the coin lands on its edge.

In analyzing data and decision making, most managers should consider and use probabilities. If you do use probabilities, you should be concerned with two situations: (1) the case where one event or the other will occur, and (2) the case where two or more will occur.

Another very important element of analyzing data (in addition to probabilities) is forecasting. Every manager considers some kind of forecast in every decision that he or she makes. Some of these forecasts are quite simple. Take the case of the operations manger who, on Thursday, forecasts the workload she anticipates for Friday in order to give one of her security officers time off. Other forecasts are more complex and usually involve long periods of time, cost, and government regulation of some future issue.

No one forecasts with accuracy; nevertheless, decisions must still be made every day and they are made with the best information that is available.

Forecasting Processes

Whether you use one forecasting technique or another, the forecasting process stays pretty much the same.

1. Determine the objective of the forecast. (What is its use?)
2. Select the period over which the forecast will be made. (What are your information needs over what time period?)
3. Select the forecasting approach you will use. (Which forecasting technique is most likely to produce the information you need?)
4. Gather the information to be used in the forecast.
5. Make the forecast.

Forecasting Types

There are three basic types of forecasts: judgmental forecasts, extensions of past history, and casual forecasting models.

Judgmental Forecasts

We tend to use these kinds of forecasts when "good" data is not readily available. With a judgmental forecast, we are trying to change subjective opinion into a quantitative forecast

that we can use. The process brings together, in an organized way, personal judgments about the process being analyzed. Essentially, we are relying primarily on human judgment to interpret past data and make projections about the future.

Extensions of Past History (Also Called Time-Series Methods)

When we take history as our beginning point for forecasting, it doesn't mean that we think October will be just like August and September; it simply means that over the short run, we believe that future patterns tend to be extensions of past ones and that we can make some useful forecasts by studying past behavior.

Casual Forecasting Modes

If considerable historical data are available and if we know the relationship between the variables we want to forecast and other variables we can retrieve, it is possible to construct a casual forecast. This model is an example of forecasts, which relate several variables.

Let's take a look at how we might use our decision-making skills and analysis of data in an exercise.

Inventory Exercise

For many security organizations, the inventory figure is an extremely large asset. Inventory difficulties can and do contribute to a business' poor image, lack of authority and control, and sometimes to the ultimate, failure. In this exercise, hopefully you will be able to see that skillful inventory management can make a significant contribution to the security operation.

There are two basic inventory decisions managers must make as they attempt to accomplish the functions of inventory:

1. How much or rather how many items to order when the inventory of that item is to be replenished.
2. When to replenish the inventory of that item.

When to order decisions (consider):

a) Lead time
   If you are calling for home delivery of a pizza and it takes 30 min or less for it to arrive, then 30 min is the lead time for ordering.
b) Lead time demand
   Consider how many pairs of gloves, seasonal items, winter coats, or short-sleeve shirts you will need to have in stock, then when stock reaches a certain point, when to order.
c) Stockouts
   Have a contingency plan. Demand of items will continue even in terrible weather (flood, snow, and hurricanes), strikes, or transportation disasters. Consider them all and plan accordingly.
d) Safety stock
   Hold out some extra items, just in case. The term safety stock refers to extra inventory held as a hedge, or protection, against the possibility of a stockout. It is, however, always part of the total inventory.

Inventory level with constant demand and lead time.

Graphic Presentations

Columns of numbers have been known to evoke fear, boredom, apathy, and misunderstanding. While some persons seem to "tune out" statistical information presented in tabular form, they may pay close attention to the same data presented in graphic or picture form. As a result, you may want to use graphs as opposed to tables. Here are two very basic examples of how to illustrate your results:

1. Pie chart: One of the simplest graphic methods. A circular graph whose pieces add up to 100%. Pie charts are particularly useful for visualizing differences in frequencies among a few normal-level categories.

Pie charts provide a quick and easy illustration of data that can be divided into a few categories.

2. Bar graphs: The bar graph (or histogram) can accommodate any number of categories at any level of measurement and, therefore, is more widely used.

In summary, graphic presentations of data can be used to increase the readability of your findings.

Determining Correlations and Causality

The statistics so far discussed have focused primarily on managing a business and monitoring staff. For any organization, these forms of statistics can reduce costs, as well as increase productivity and efficiency. However, when security enters into the equation, we can also turn to social statistics to provide additional information. For example, a retail loss prevention specialist might be interested in which demographic characteristics are most related to shoplifting. Or, perhaps, statistics could provide the specialist with clues to the optimum balance of accessibility for customers to reach an item and added security to prevent shoplifting. An item locked behind glass is less likely to be stolen, but also less likely to be purchased. How much security is too much security? Statistics from prior experimentation could provide answers.

Before getting too involved into these statistics, the purpose of this discussion should be made clear. This introduction to correlations and causality is intended to provide the reader with enough information to understand the importance and the underlying principles of statistics, as well as a meaningful way to interpret these statistics. Those interested in collecting data and analyzing it should consult additional sources relating to research methods, correlation, and regression. The *Statistics Package for the Social Sciences* (SPSS) is presently a commonly used software package well suited for this kind of analysis.

There are several terms used in statistics that must be defined before delving deeper into the topic. A *variable* is something that can change or otherwise varies from person to person. An *attribute* is one of the possible characteristics within a variable. For example, sex is a variable, while male is an attribute. Similarly, height is a variable, while 5′11″ is an attribute. In other words, a variable is a category and an attribute is some characteristic or measurement that falls within a given category. An *independent variable* is the cause in a relationship (or more precisely, the variable believed to be the cause) and a *dependent variable* is the outcome or effect in the relationship. A *correlation* is a relationship between two variables. It can be positive in which having a high attribute with one variable is usually associated with a high attribute with another variable. For example, among children, a higher age is usually associated with a higher level of intelligence. This is a positive correlation. By contrast, a correlation can be negative. Education and shoplifting could be an example of this. Hypothetically, a higher number of years of education could be associated with a lower likelihood of shoplifting and vice versa. In simple words, a correlation indicates that there is some sort of a relationship between two things. If you know only one attribute of a person or thing, you would be able to make a reasonable guess as to a second attribute if a correlation exists.

A correlation, however, does not necessarily denote causality. To prove something caused something else, there are three requirements that must be met:

1. There must be a correlation between the cause and the effect
2. The cause must occur before the effect
3. The relationship must be not the result of a third variable

It is the final requirement that is often most difficult to establish. In statistics, a relationship caused by a third variable is called a *spurious* relationship. An example of this could be found with shoe size and criminality. If we only looked at these two variables and claimed

to have found causality, we would likely come to the conclusion that as shoe size increases, involvement in crimes also increases. There are two other variables that might account for most or all of this correlation. First, age is a factor because young children have a smaller shoe size and are less involved in crime. Second, sex has an effect on the relationship because men are more likely to be involved in crime and have a larger shoe size. Overall, a researcher would not be wrong to conclude that shoe size is related to crime, but that does not establish causality and hardly gives us the whole story. Additionally, knowing correlations can lead to useful security implications. Just because causality is not established does not mean the information is worthless.

The *experimental design* is the best way to establish causality. It is also the most effective way to test a change to procedure. In an experimental design, there must be at least two groups. The first group is the control group, which is *not* exposed to the *experimental stimulus* (the change being tested). The second group is the experimental group and it is exposed to the experimental stimulus. The results can then be compared to see if the experimental group experienced changes the control group did not. As long as the participants (people, buildings, organizations, etc.) were randomly assigned to one of the two groups, any changes observed only in the experimental group can be reasonably attributed only to the experimental stimulus. The stimulus can then be said to be the cause of the change.

This design can be difficult to understand without an illustration, so here is an example. Let's say a director of security for a chain of storage facilities with over 250 locations is interested in adding fake security cameras to deter would-be vandals. However, the organization will not authorize the expense without proof that the cameras will work. Determined to get the funding, the security director randomly chooses 25 of the locations to install the cameras (the experimental group) and does nothing to the other locations (the control group). After one year, the security director notices a decrease in vandalism by 60% at the locations with the cameras, while a drop of only 10% at the other locations. What these statistics imply is that some part of the 60%, approximately one-sixth of it, is likely caused by other changes in policy or society. However, the majority of the decrease was unique to the locations with cameras and therefore is the proof needed to acquire the additional funding. Testing the medicinal purposes of new drugs is a similar process. A random selection of participants (the experimental group) is given the drug and the remaining participants (the control group) is given a placebo. This is an extremely effective design, as care is taken to make sure people involved in both groups believe they are in the experimental group. In the storage facility example, it is possible even with an experimental design for a third variable to be involved. Security officers, for example, might have increased patrols believing they were being watched if they were not informed that the cameras were fake. Likewise, had the vandalism rates increased, the officers might have decreased patrols relying on the fake cameras to deter.

Using statistical *controls* is sometimes the best option for establishing causality if an experimental design is not feasible. These controls are simply additional variables added to the equation. As more controls are added, the impact of the independent (cause) variable on the dependent (effect) variable will decrease, but any conclusions will become more valid and accurate. A study by the Census Bureau in 1987 illustrates the usefulness of this approach. It is a well-established fact that women make less money than men overall in the United States When one reads this, one almost instinctively assumes there is a causality involving discrimination behind this relationship. However, once other variables are added (years on the job, marital status, type of occupation, education level, and many others), 60% of the difference between the income of men and women can be explained through other nondiscriminatory factors. This does not negate the fact that women make less than men, but it does partially explain it and increase our understanding of the problem. The remaining unexplained difference could similarly be explained by adding additional variables. Likely, an additional portion would be explained if enough variables were added, while some would remain unexplained by legitimate reasons for pay differences.

When a researcher believes that more than one cause exists, as is virtually always the case in social statistics, *multiple regression* can be used. Rather than testing each relationship separately, regression allows each possible cause to be tested simultaneously. For example, delinquent peers and frequently witnessing crimes both correlate with delinquency. However, because

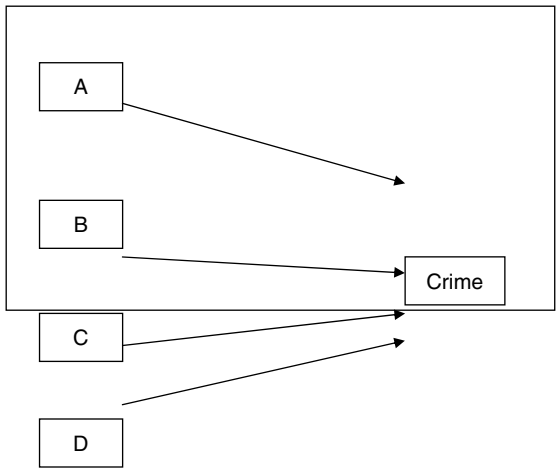


FIGURE 2.1 Regression.

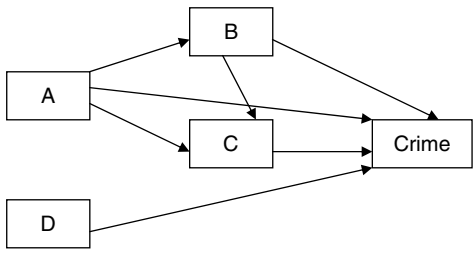


FIGURE 2.2 Path analysis.

the two concepts are not unrelated (having delinquent friends will likely increase the amount of crimes witnessed), the two relationships should be tested together. This allows for the overlap in the concepts to be controlled and generates more accurate statistics (Figure 2.1).

There are other more advanced forms of statistics that have only recently become possible due to advances in computer technology. Path analysis, for example, allows us to track causality through mediating variables. While in previous years we might have just tested whether being around delinquents increases delinquency, today we can test whether it also increases prodelinquency beliefs and abilities and whether those have an impact on delinquency. These essentially allows us to statistically test a flow chart. See Figure 2.2 for an illustration.

Conclusion

Whether trying to influence people or justifying your operating budget, look to your everyday experiences as data. Use that information to make predictions about future events and use statistics as an aid in testing your predictions. As with many managerial tasks, there is uncertainty and the use of statistical analysis is no exception. However, utilizing the probability theory and forecasting methods along with simple mathematical formulas and percentages will add authenticity to your decisions and confidence in your conclusions. Statistics can be easily combined with virtually any other area of interest as well. For example, quantifying turnover

rates and costs can help illustrate a potential problem. The financial impact of turnover (and various other problems) can be communicated more clearly when statistics are used to define and summarize problems. You can also turn to others' experience and research to provide additional information. From industry-specific research to theory testing by criminologists, useful and informative statistics are plentiful.

Statistical Analysis

Quiz

1. Statistical analysis is the methods and processes used in obtaining _____ and the methods and means for estimating their reliability.
2. _____ and _____ are the key elements in the analysis phase of information gathering.
3. Events are _____ if one and only one of them takes place at a time.
4. The time-series method of forecasting is also called _____.
5. In _____ forecasting, you are relying primarily on human judgment to interpret past data and make future projections.
6. The waiting lines or queues are a problem for a manager because the manager must balance the increased cost of more help against customer complaints.
   ☐ T ☐ F
7. Probability is the chance that something will happen.
   ☐ T ☐ F
8. Which of the following is required for proving causality?
   a) A correlation
   b) A time order
   c) A nonspurious relationship
   d) All of the above are required
   e) Any of the three is sufficient evidence
9. An experimental design involves at least four groups that require careful assigning of individuals to the group most suitable for their individual needs
   ☐ T ☐ F
10. Statistical controls:
    a) Should be avoided because they decrease the prediction power of other variables
    b) Are unnecessary in most analyses
    c) Help establish causality and clarify relationship
    d) Are always used in all analyses

This page intentionally left blank

3 Security Technologies*

Henry C. Ruiz

Introduction

As we enter the twenty-first century, our roles as protection officers are changing at a tremendous rate, particularly where the use of information technology-based hardware, such as computers, and software that permits multitasking, asset tracking, and critical response is involved. To be more effective, protection officers must be well versed in the use of high technology tools.

High technology has influenced our profession and will continue to do so. In our profession high technology is primarily used in electronic access control systems, closed circuit television (CCTV) systems, fire safety/life safety systems, and nonsecurity systems monitored by protection personnel. With the computer as a baseline tool, high technology has changed and enhanced our profession with the concept called Security Systems Integration and Convergence. Security Systems Integration is a concept that all protection officers must be familiar with. Convergence is the melding of other information technology-based systems with security systems.

Security Systems Integration

In the past our roles as protection officers were primarily concerned with the issues of access control and physical security. These roles were limited. As such, we were perceived as unskilled persons whose main functions were to guard gates and shake doors. This changed with advances in technology. Specifically, what affected our profession was the invention of the personal computer. This enabled many security tools, such as alarm systems, access control systems, and CCTV systems, to be developed or improved on.

For many years the security industry was divided into security guard services and alarm services. They were perceived as being separate functions. Today, our roles and what we do go far beyond these functions. We provide many services to our customers beyond access control and physical security. We are total protection professionals. With the advances in technology, electronic access control systems, CCTV systems, fire safety/life safety systems, and related systems, we protection professionals can now meet the needs of our customers more effectively with more tools to work with. This is what is called Security Systems Integration. For the protection officer, the definition of Security Systems Integration is as follows: The unification of computer-based security and related systems into one overall system that is controlled by the operator and meets the needs of any situation.

Computer Basics and Enterprise Systems

High technology tools affect everything we do. To increase our professional skills, and in fact survive in the twenty-first century, we must master these tools. The most important tool and

* *Updated in 2007 by Jeffrey A. Slotnick, PSP*

the baseline of Security Systems Integration is the computer, more commonly called a work station, handheld computer, or mobile computer (laptop).

Computers in Security Operations

Computers have many applications in security operations. As a minimum, they are used to control and monitor electronic access control systems, CCTV systems, fire safety/life safety systems, and security management systems, including patrol tour systems, officer scheduling, parking lot control, key control, other physical security systems, and incident reporting and investigation management systems. More and more computers are becoming primary tools in security operations. They are easy to use and make the protection officers more effective in their day-to-day duties.

What is a Computer?

A computer is an electronic-based device or appliance that can perform complex computations, gather data, provide information in data or picture (graphic) form, and control various systems including those used in security operation. More importantly computers have the capability of communicating with each other in an enterprise using a principal computer called a server. The server also permits collaboration through workgroups.

Personal Computer Hardware

Console: A PC console is basically a plastic and metal box containing the computer. It can be in the shape of a flat rectangular box called a "desk top," in a vertical form called a "tower," or in a takeaway or portable model called a laptop. On the back of the console are connections called "ports" to which are attached various kinds of hardware, including the monitor, keyboard, and printer. In the front of the console is the on/off switch or button and status lights that indicate when the computer is on and at least two horizontal slots for compact discs (CDs), digital video disks (DVDs), or, most recently, a number of devices that connect utilizing a Universal Serial Busport (USB). The use of a USB allows for connection, download, and synchronization of memory storage devices, cameras, handheld computers such as a Palm Pilot, or numerous other devices. Inside the console are the basic components of the computer. The most important components are the microprocessor, random access memory (RAM), hard disk drive, cable modem, or wireless connection. A brief description of each follows:

Microprocessor: The microprocessor is the most important part of a computer. It is the brain of the computer and controls the flow of information throughout a computer system. Because of the miracles of high technology, the microprocessor is housed in a tiny microchip no larger than a dime. The performance and power of a microchip is based on clock speed, which is measured in the electronic measurement of megahertz (MHz) A megahertz is equivalent to one million electrical vibrations per second. The higher the megahertz, the more powerful the microprocessor is. The microprocessor is also called the central processing unit or CPU.

Random Access Memory: RAM is the second most important part of a computer. RAM is where computers temporarily store information while they are in use. RAM is like an electronic work area where you store your work items. RAM is measured in the electronic measurement of gigabytes (GB). Most personal computers need at least 1 GB of RAM to function effectively.

Hard Disk Drive: To permanently store software programs and other information, the computer uses magnetic-based disks to store information. These disks are stored in devices called drives. The primary kind of disk is called the hard disk drive and is stored in the computer console. A hard disk drive or hard drive contains several disks. These disks rotate very quickly and the information stored on them is read by special heads that can also write data onto these disks. Green, red, or yellow lights on the front of a PC console let you know when the drive is in use. Hard drives store an enormous amount of information from 60 GB on the low end to servers that store data measured in terabytes.

Universal Serial Bus Ports: On most computers there are numerous high speed communication ports for attaching a multitude of devices including printers, cameras, scanners, card readers, and portable memory sticks to name a few.

CD-ROM, DVD ROM, and CD/DVD RW: Most computers have a CD or DVD-ROM drive to accommodate CDs and DVDs. Currently there are three competing technologies for rewritable DVDs: DVD-RAM, DVD+RW, and DVD-RW. DVD-RAM is considered a highly reliable format for traditional computer usage tasks such as general data storage, backup, and archival. The on-disc structure of DVD-RAMs is closely related to hard disk and floppy disk technology, as they store data in concentric tracks. DVD-RAMs can be accessed just like a hard or floppy disk and usually without any special software. DVD-RWs and DVD+RWs, on the other hand, store data in one long spiral track and require special packet reading/writing software to read and write data discs. These discs can hold upwards from 1 to 5 GB of information depending on the format. They are extremely useful for such applications as animated graphics, sound, and video. These applications are certainly used in security operations.

Cable Modem or Wireless: Computers use telecommunications technology quite extensively, particularly with the use of the Internet. To use telecommunications systems, the computer must be able to communicate with these systems. This is accomplished with the use of a device called a cable modem, T-1 connection, or wireless connection that communicates data through fiber optic and other high speed communication lines. As many applications and devices need to communicate with the Internet to operate a connection of this nature is highly desirable and required.

Other Computer Hardware: As mentioned earlier, other major hardware includes the monitor, keyboard, printer, and mouse. These and other hardware not actually inside the PC console are called peripheral devices. A brief description of each follows:

Monitor: The monitor is very similar to a television set but does more. Monitors have to display a clear and crisp display of text in addition to moving images. Monitors are also configured to produce sound to accommodate what is called "multimedia" applications that enable one to interact with a computer more effectively.

Keyboard: The keyboard is the primary input or entry device for a computer. Similar to a typewriter keyboard, it has many functions. Composed of at least 110 keys, the keyboard controls the functions of a computer, including entering/deleting data, calculating, and control functions.

Printer: The printer is the primary output device for a computer. The printer produces output in the form of hard copy paper text, graphs, and photographs. Printers come in various shapes and sizes and produce copy of varying degrees of quality.

Mouse: Another major input device is the mouse. A mouse is usually a small control device connected to the computer via a cord or, in some cases, wirelessly. Its shape and cord make it look like a mouse. A mouse performs many functions more effectively and efficiently than a keyboard, particularly control functions. It is a major tool for the computer user.

Peripheral Devices Applicable to Security Operations: Many computer-based security application systems have peripheral devices attached to computers. The most common are badge and identification units used to take photographs and data recorders used in computer-based or bar code-based patrol tour systems.

Personal Computer Software

When you turn on a computer it will activate most of its components. This process will show up on the monitor as the computer starts up. The system will be ready to use when the computer's "operating system" is activated. The operating system is the software that actually tells the computer what to do. Today, the most widely used operating system is Windows. Windows and its various versions are very easy to use and very flexible. By itself, Windows offers the user many features including word processing, data management, and system controls. Although Windows and its various versions offer the user many options and capabilities, a computer will also accommodate other software called "application software." The amount and subject matter of application software is vast. Included are software packages for word processing (Microsoft Word), database management (Microsoft Access), presentation software (Microsoft PowerPoint), spreadsheet analysis (Microsoft Excel), and many others with specific applications that support investigations, project management, and accounting. The

number and subject matter for security operations used is also extensive and many products are on the market. Many of you work with them. With a computer you can prepare incident reports, manage and analyze information, make decisions, and control sophisticated systems including most security and security-related systems. In general, a computer enables you to perform your duties more effectively and efficiently.

How Computers are Used in Security Operations

In security operations computers are commonly used to control and monitor electronic access control systems, video systems, alarm systems, and other security-related systems that are in an integrated environment where all systems work together and communicate with each other. For example, the most widely used security operation controlled and monitored by computers is alarm monitoring of intrusion alarms. A typical system consists of a computer, as described earlier, connected to controller systems at alarmed areas or points via telecommunications lines. Alarmed points and areas are programmed and stored in the computer. The alarmed points and areas are displayed on the computer's monitor in graphic form, such as maps, diagrams, video, digitized photographs, or alphanumerically. The computer and alarmed points/areas communicate and are continuously monitored by the system controllers. The computer operator has the capability to monitor alarms with various features built in to the alarm monitoring software for the system. When the operator wants to monitor an alarm point or area, the operator enters an instruction into the computer using the keyboard, mouse, or peripheral device unique to the system. This instruction activates the computer's CPU, which reports the alarm status on the monitor and on hard copy using the printer. When an alarm occurs, it is displayed on the monitor, recorded in memory by the CPU, and printed on hard copy. Most systems also display instructions concerning how to respond to alarms.

How and Where to Learn More about Computers

To become a more effective protection officer, it is to your benefit to learn all you can about personal computer systems. More opportunities will be available to you and you will add more value to your employer if you are computer literate. Indeed, the trend is toward high technology. There will be fewer opportunities for traditional protection officers as we know it. The protection officer of the future will be a unique professional with a high-level skill set and knowledge base including an effective command of computers and related systems.

There are many ways to become better educated in computer systems. Many courses and training opportunities are available to learn about computers, primarily at the vocational and junior college level. There is a vast amount of literature dealing with computers in libraries and bookstores. You are also encouraged to get your own computer since one of the best ways to learn about computers is to use them.

On the job always seek opportunities to use computers. The best opportunities are in security control operations, security administration, security database management and the maintenance of computer systems, and computer-based security application systems.

Electronic Access Control Basics

Access control is a security method that controls the flow of traffic through the access points and areas of a protected facility. Access control is one of the primary functions of protection officers. The key element of access control is identification. This can be accomplished by having officers posted at access points and areas, using CCTV systems, biometric systems, and electrical/mechanical controls, or by using computer-based electronic access control systems.

What is Electronic Access Control?

Electronic Access Control (EAC) is a method of access control that uses computer-based technology to control and monitor access. Most EAC systems use credit card sized access control cards that are programmed to actuate devices called card readers. These card readers are installed at controlled locations, entry portals. In a typical system, the individual presents his or her card to a card reader at the controlled location. The location could be a door, turnstile,

gate, or other access point or area. The card reader's sensor extracts information from the card and translates that information into a code number and sends this information to the system's computer. This number is compared with the user's programmed access information and access is either granted or denied. When access is denied, an alarm may be activated, depending on the system. In most cases, there may be a record of each access transaction. This provides the system's basic audit trail.

The Basic EAC System

The following describes a basic EAC system:

Access Cards

Proximity Cards Proximity access cards are the most widely used for EAC systems. They work via the use of passively tuned circuits that have been embedded in a high grade fiberglass epoxy card. To gain access, the cardholder holds or presents the card within 2 to 4 in. from a card reader. The reader's sensors detect the pattern of the frequencies programmed in the card. This pattern is then transmitted to the system's computer. If the pattern matches the reader's pattern, the reader unlocks the door and records the transaction. If the pattern does not match, no access is granted and this information is recorded and an alarm may be activated.

Magnetic Cards Magnetic cards use various kinds of materials and mediums to magnetically encode digital data onto cards. To gain access, the card user inserts or "swipes" (passes the badges through) the card through a slot in the card reader. As the card is withdrawn from the reader, it moves across a magnetic head, similar to that of the tape recorder head, that reads the data programmed in the card. The information read from the card is sent to the system's computer for verification. If verification is made, the computer sends a signal to the card reader to grant or deny access, and if access is granted, the door is unlocked.

Magnetic cards look like credit cards. The most popular medium for this type of access card is magnetic stripe. With this type of card, a pattern of digital data is encoded on the card's magnetic stripe. This type of card is relatively inexpensive and a large amount of data can be stored on the magnetic stripe that is placed on one side of the card. Magnetic cards tend to chip and break, however, through excessive use. Another type of magnetic card medium uses very small dots of magnetic materials that are laminated between plastic layers of the card. This type of card is cheaper to use than the more widely used magnetic stripe card, but is subject to vandalism and wear and tear.

Weigand Cards Weigand-based access control cards use a coded pattern on magnetized wire that is embedded within the card. When this card is inserted into a reader, the reader's internal sensors are activated by the coded wire. This type of card is moderately priced and will handle a large amount of traffic. It is less vulnerable to vandalism and weather effects than other types of cards. Its main deficiency is that it is subject to wear and tear.

Other Types of Access Cards **Smart cards** contain an integrated chip embedded in them. They have embedded coded memories and microprocessors; hence, they are like computers. The technology in these cards offers many possibilities, particularly with proximity-based access systems.

Optical cards have a pattern of light spots that can be read by a specific light source, usually infrared.

Capacitance cards use coded capacitor-sensitive material that is enclosed in the card. A current is induced when the card activates a reader. This current checks the capacitance of the card to determine the proper access code.

Some access devices come in the shape of keys, disks, or other convenient formats that provide users with access tools that look attractive and subdued but at the same time are functional.

Card Readers

Card readers are devices used for reading access cards. They come in various shapes, sizes, and configurations. The most common reader is the type where the card user inserts the card in a slot or runs or swipes the card through a slot. The other type of reader uses proximity technology where the card user presents or places the card on or near the reader.

Some insertion-type card readers use alphanumeric or numeric keypads where after the user inserts the card, the user enters a unique code number on the keypad. This action then grants access.

Biometric Access Control

As we enter the twenty-first century, biometric technology or the use of human biological characteristics for identification and verification is increasingly being used in access control systems. The most popular systems use hand geometry, fingerprints, palm prints, eye retinal patterns, voice prints, and signature recognition. When biometric devices are used, they are designed and installed concurrently with card reader systems.

EAC System Applications

An EAC system is ideally used as part of a fully integrated facility management system. In such a system, EAC is interfaced and integrated with CCTV systems, fire safety/life safety systems, communications systems, and nonsecurity systems such as heating, ventilation, and air conditioning systems.

In an integrated system, EAC systems allow users access into various areas or limit access. They can track access and provide attendance records. As a safety feature and for emergency response situations, they can determine where persons are located in facilities. In general, EAC systems are flexible and strides in technology are making them even more so.

CCTV Systems Basics

CCTV systems are among the most effective high technology tools for protection officers. They extend the "eyes" of protection officers and thus enhance the observation and reporting skills of protection officers. CCTV systems range from simple camera and cable systems to sophisticated and complex systems using various technologies and having many applications.

CCTV Equipment and Components

A basic CCTV system consists of a camera, monitor, transmission medium, control equipment, and recording devices. A brief description of each follows.

Camera

The camera used in modern CCTV systems is based on integrated circuit technology, which uses an array of solid state light-sensitive elements called pixels arranged on a silicon chip to sense light passed from the scene being televised through the camera's lens. The light passed by the lens falls on the camera's sensors. These sensors release electrons proportional to the intensity of the light striking the pixels. This electron stream is flexible depending on the camera configuration. The most popular type of camera is called a charged coupled device camera. This type of camera is extremely powerful and comes in various shapes and sizes depending on its deployment. Cameras will record images in color or black and white depending on the need. Cameras can be coupled with infrared lighting to provide night time observation.

Monitor

The monitor displays the transmitted picture from the camera. The picture quality is similar to very advanced television systems. The picture can be displayed entirely on the monitor screen or via multiple images in a split screen format.

Transmission Medium

The CCTV camera generates a signal to be transmitted as a picture to the monitor by various mediums. The most widely used are coaxial cable, optical fiber, twisted wire pair, microwave, and wireless technologies.

Control Equipment

Most CCTV systems require control equipment for various purposes. Included are control mechanisms for controlling cameras, transmission mediums, focusing, and lighting. Major control equipment for CCTV systems are multiplexers that enable multiple cameras to be used on one single system, signal processors, signal sequencers, video motion detectors, lens controls, switches, and pan and tilt devices that control the movement of cameras.

Recording Equipment

An older technology uses video recorders (VCRs) similar to those used for standard televisions. VCRs for CCTV systems have more advanced features than the typical VCR because of the information they record. VCRs record in real time or time lapse, which is slower than real time, but is more useful for security uses. Most VCRs record the time and date, which is essential for security needs.

Most recently many systems are formatted using digital video recorders (DVRs). DVRs use the same technology as a hard disk drive on your computer and here is an overview of that technology.

Key factors that contribute to the quality of images taken and recorded to DVR are as follows:

1. **Camera resolution**: This is one of the important specifications to consider when considering a security camera as it could make the difference in identifying a person committing a crime by having the highest resolution. The more lines of resolution the higher the definition of the picture. Indicated by the number of horizontal TV lines that make up a picture each individual horizontal TV line is made of a number of pixels and the total number of these lines makes up the full picture you see on your screen.

   What resolution is available in the market for security color cameras?

   –800 TV lines 3 CCD camera
   –600 TV lines Television Broadcast
   –550 TV line s Newer 2005 models
   –470/480 TV lines “High Resolution”
   –420 TV lines “Medium Resolution”
   –380 TV lines “Standard Resolution”
   –330 TV lines “as seen in toys and hobby cam”
   –100 TV lines “as seen in web cam”

When choosing security cameras and security camera systems you must consider the resolution and application of each individual component comprising your security camera system so you can select components with similar resolution.

2. **Recording resolution of your recorder:** A DVR, meant for security surveillance and mission-critical applications, is a sophisticated system composed of specialized hardware, software, and subassemblies with built-in checks and balances. It all must work in unison to create a robust and reliable piece of equipment.

   Recording Resolution: Do not confuse it with Viewing (live) Resolution

   –800 × 600 “mission-critical application”
   –720 × 480 “Highest resolution for commercial”
   –720 × 240 “Mid Resolution”
   –640 × 480 “State Gaming (casino) Commissions Standard”
   –320 × 240 “Standard Resolution”—as seen in most DVRs
   –160 × 120 “Low Resolution”—storage savior
   –80 × 60 “web cam resolution”

CCTV Applications

CCTV applications are only dependent on the needs, creativity, and pocketbook of the end user. Most CCTV systems are used to monitor sensitive areas requiring surveillance. For example, a common application of CCTV is to supplement patrol operations by monitoring perimeter areas that cannot be patrolled continuously.

An integrated system, CCTV has vast potential and uses. For example, in an access control application, when the access control system registers an alarm, it will signal the CCTV system to pan the area causing an alarm. The system's monitor will then show what is going on in the area, whether its trespassing, burglary, or other situation. CCTV systems will also assist other components of an integrated system. In a fire safety/life safety situation, the CCTV system could be integrated with certain fire alarm systems and provide an image of an area being affected by fire. This assists first responders in assessing the situation safely without sending the person into harms way.

Fire Safety/Life Safety and Nonsecurity Systems

Security operations have evolved from basic guard operations concerned only with physical security and the protection of material assets to having responsibility for various areas not traditionally associated with security. As a minimum, this includes fire safety/life safety systems, facility environmental systems, and the monitoring of process controls for nonsecurity areas such as manufacturing and laboratories. This concept of having security responsible for monitoring nonsecurity systems is called total facility control (TFC). In TFC, various aspects of a facility are connected to security systems via systems integration technology to provide total control over a facility and greater safety and comfort for facility occupants and users. Each area of TFC is summarized as follows.

Fire Safety/Life Safety Systems

The major components of fire safety/life safety systems include sprinkler systems, smoke detectors, duct detectors, and heat detectors. In an integrated environment these systems are monitored and controlled at a centralized location by security personnel. Monitoring personnel have total control over these systems. They can override or shunt them for various purposes and alarms can be responded to more efficiently and effectively when combined with other systems. For example, a fire in a certain location will set off evacuation alarms, turn on a sprinkler system, lock certain doors to contain a fire, and provide the exact location of the fire so it can be responded to by firefighting personnel. With conventional systems, most of these functions would be executed separately and not interact with each other in a real time manner. In an integrated environment they would occur simultaneously or in real time.

Environmental Systems

In an integrated environment security personnel monitor and in certain cases respond to problems and situations involving environmental systems. Environmental systems include energy management via heating, ventilation and air conditioning systems, lighting, elevator systems control, and the control of power systems. These systems ensure that facilities are operating efficiently and providing a safe and comfortable environment for occupants. This applies to both buildings and campus facilities.

In an integrated environment, if a system is malfunctioning an alarm or signal will register on the system control monitored by security personnel. Depending on the type of control system used, the situation can be handled by security or dispatched to the appropriate facility maintenance personnel. For example, a common situation is a power outage or a power surge where the power needs of a facility may be interrupted. In a conventional system the common approach is to inspect every system affected and reset applicable systems. Notification of affected personnel must also be made. This takes time and involves many persons to respond. With an integrated system, systems

can be reset from a centralized location (usually the control center) and notification can be made by telecommunications systems connected to the overall system. This saves time and labor costs.

Monitoring Process Controls for Nonsecurity Areas

The monitoring of process controls involves the profit end of an entity, either concerned with manufacturing/production or research and development. Monitoring process controls includes such systems as freezers, refrigerators, incubators, laboratory systems, water purification systems, and manufacturing and production processes.

In a converged environment these systems can be connected to security control centers and monitored on specially designed systems. If a process control system alarms, security personnel can assess the situation and notify the proper persons to respond. The monitoring of process controls is value added because security is contributing to the bottom line of profit that these systems are generating. Additionally, operational controls can be used to determine breaches of security; for example, a loss of pressure alarm could be a legitimate leak or it could be an indicator of vandals illicitly opening a valve. In another instance, a hatch alarm on a water tank that is opened during off hours could indicate a potential attack on critical infrastructure.

How and Where to Learn More about Security Systems Integration and High Technology Tools

There are many avenues and opportunities for the protection officer to learn more about security systems integration and high technology tools. The best way to learn about these areas is through hands-on experience, training, and taking advantage of educational opportunities that are available through the following:

- Many security equipment manufacturers have travelling road shows to educate users on their products. Pelco and Ademco are two major distributors that host this type of training.
- Vocational schools offering courses in computer technology, electronics, and related areas.
- Junior colleges offering courses in high technology areas.
- Computer and high technology courses offered by one's employer.
- Job opportunities and assignments involving personal computers, systems integration, and high technology tools. Included are Control Room Operator, Security Systems Technician, and Security Specialist positions.

The information base concerning Security Systems Integration and high technology tools is vast, so be prepared for extensive study. The following references will provide you with a start.

Bibliography

Security, ID Systems and Locks: The Book on Electronic Access Control by Joel Konicek and Karen Little; Butterworth-Heinemann, 1997. This is a very user friendly book about electronic access control.

Total Facility Control by Don T. Cherry; Butterworth, Stoneham, MA, 1986. This book describes in extensive and simplified detail the applications of security systems integration in relation to total facility control.

Access Control and Security Systems Integration. This is an excellent trade magazine and professional journal dealing with high technology security and related systems. It provides the latest information about access control and security systems integration. Address: 6151 Powers Ferry Road NW, Atlanta, GA 30339-2941.

More information about the above and other references can be obtained from the International Foundation for Protection Officers.

Security Technologies

Quiz

1. Security Systems Integration is the _____ of _____ security and related systems into one overall system that is controlled by the operator and meets the needs of any situation.
2. Protection officers do not need to be concerned about high technology areas such as security systems integration and high technology tools that assist the protection officer. ☐ T ☐ F
3. A _____ is a device that can perform complex computations, gather data, provide information in picture form, and control various systems.
4. Computers have many applications in security operations. ☐ T ☐ F
5. _____ is a _____ method that controls the flow of traffic through the access points and areas of a protected facility.
6. The key element of access control is identification. ☐ T ☐ F
7. A _____ consists of a camera, monitor, transmission medium, control equipment, and recording devices.
8. Proximity-based electronic access control systems are inefficient, ineffective, and are the least used access control system. ☐ T ☐ F
9. The concept of having security responsible for _____ nonsecurity systems is called _____.
10. Closed circuit television systems are among the most effective high technology tools for protection officers. ☐ T ☐ F

4 High-Technology Theft

Cole Morris

Theft in the workplace has been a concern for decades. In fact, the prevention of theft of organizational property has always been a primary responsibility of the private security professional. Not too surprisingly, the advances in technology and the global spread of electronic and digital devices have raised the bar to a new level. We are no longer simply concerned about the "misappropriation" of a box of pencils or ream of paper. Today's security supervisor must also be concerned about the possible theft of computers, personal digital assistants (PDAs), cell phones, storage devices, printers, digital projectors, and a host of other assets used to support business goals.

This chapter will contribute to your awareness of this threat by discussing the following:

- Motivations for high-technology theft.
- Technological and social trends contributing to this crime.
- The cost of high-technology theft.
- Security countermeasures.

It is important to remember that it makes little difference what type of environment you are working in. The incredible spread of technological devices has resulted in these high-value assets being used everywhere from office suites and libraries to schools, hospitals, government buildings, and just about any place else you can imagine.

New Concern: Identity Theft

In the previous edition of *Security Supervision*, focus was placed on the economic impact that high-technology theft had on the workplace. This impact continues to grow and has been supplemented with a major new concern: identity theft.

Consider these recent events:

- *A laptop computer from the inspector general's office at the Department of Transportation was stolen last month, putting the sensitive personal data of nearly 133,000 Florida residents at risk…*
- *Employees arriving for work Tuesday at the Sterling Bank office building on Carmichael Road received a shock when they found that burglars had made off with more than 20 laptop computers from businesses in the building…*
- *Two teenagers were arrested Saturday in the theft of a laptop computer and hard drive containing sensitive data on up to 26.5 million veterans and military personnel…*

In many instances, identity theft is not the primary objective of the thieves. Often they seek high-value items for their monetary value. However, the fact that a stolen device can even *potentially* be used to conduct identity theft is a serious problem. With high-profile incidents and wall-to-wall media coverage, organizations can ill-afford the negative publicity involved with even the *possible* theft of personal information. This is easy to understand. Such incidents shake the confidence of customers and clients. Stakeholders question the competence of management. Claims are often made of "negligence" and breach of trust.

In short, even the *potential* loss of personal information means you are not likely to have a good day.

Proprietary Information

Although identity theft is grabbing all the headlines, you also need to realize that the loss of high-technology assets can result in serious, if not catastrophic, loss of proprietary information. This can include anything from strategic business plans, customer lists, marketing initiatives, trade secrets, and similar sensitive documents. Essentially, proprietary information is information "owned" by the organization; it is information that gives you a competitive advantage in the marketplace. As you can imagine, the loss of such information can have a serious impact on any organization.

Some Things do not Change

In addition to the potential value of personal and proprietary information, many thieves are simply motivated by greed and the promise of some quick cash. For example:

- *A computer maintenance worker at a suburban school district pleaded not guilty Thursday to charges he stole nearly three dozen PCs and other equipment to sell over the Internet, earning as much as $25,000 in the process…*
- *Detectives reported the van was burglarized and computers, hard drives, and digital projectors valued at $30,000 were taken…*
- *The investigation by corporate security revealed the employee would enter the facility on weekends and take laptops from unoccupied workstations…*

Thus, thieves can have several motivations for engaging in high-technology theft and today's security supervisor must be prepared to meet the challenge.

Recent Trends

Several technological and social trends are contributing to the growth of high-technology theft. Keep the following in mind as you consider the protective plan:

Growing prevalence of these assets in all types of work environments increases their chances of being targeted by thieves. Dropping prices and wider availability of computers, cell phones, digital cameras, PDAs, and similar devices only mean they will become more widely used.

Smaller sizes of these business tools make them easier to transport, conceal, and possibly steal.

Increased storage capacities combined with miniaturization means that more and more data can be kept on smaller and smaller devices. For example, a USB drive the size of a human thumb can now hold the personal information of hundreds of thousands of individuals.

Multi-purpose devices can now perform multiple tasks. This means a single device might contain customer lists or other proprietary data, voice mail messages, telephone numbers, digital photos, and sensitive video of your latest product offering. This means the loss of one small electronic device can mean the loss of business-critical information in various formats.

Criminal awareness has increased. Thieves and potential thieves are becoming more technological savvy. They are not only discovering the "street value" of stolen assets but also are learning of the potential value of stolen personal identities and proprietary information.

Increasing convertibility means stolen assets are easy to convert into cash. In short, the neighborhood fence, flea market, and pawn shop have been supplemented with online avenues. Today's thieves do not think twice about using resources such as web pages or services such as E-Bay to "move" their ill-gotten gains. And of course, the anonymity of the Internet is ideal for such activity.

The Cost of Theft

In addition to damaged reputations, lost business opportunities, and compromised personal and proprietary information, there is obviously a direct economic loss involved with

this type of theft. In 1999, A RAND study reported that the theft of high-technology components in the United States was costing business about $5 billion each year. The report further added that of this, about $4 billion in losses could be attributed to the theft of high-technology products directly from corporate and individual users.

According to the 2006 Computer Security Institute (CSI)/Federal Bureau of Investigation Computer Crime and Security Survey, losses are increasing. The report states that average losses due to laptop and mobile hardware theft increased from $19,562 per survey respondent in 2005 to $30,057 in 2006. Of course such numbers are often just the tip of the proverbial iceberg. In any loss, you must also factor in additional costs. These can include the following:

- Increased insurance premiums.
- Lost business from not being able to meet customers needs.
- Management time having to deal with the loss.
- Cost of a temporary replacement.
- Shipping and "make ready" programming for replacement equipment.

As we can see, the loss of even one high-technology asset can significantly impact an organization at many different levels.

Basic Security Safeguards

Now that we have a better appreciation of the threat, a discussion of potential security countermeasures is in order. Not surprisingly, you will find many basic security practices effective. For example, the security supervisor should examine perimeter security of the building and make sure it includes appropriate "target hardening" features. As in all aspects of physical security, the idea is to have the criminal give up the idea of an attack, give up during an attack, or take enough time for the security force to respond to an attack before it is successful. A building's entrances, exits, and utility doors are vulnerable and should be the starting point for improved perimeter security.

As a security supervisor you may be expected to make observations recommendations to your own employer or your client's management. Keep in mind that many business people are focused on their primary profit-making activities. They may consider their building "just" an office. However, for potential thieves, the high-technology assets found there make the facility a potential gold mine. Look at your facility as a thief would and be prepared to suggest improved security as appropriate. Common methods for improving perimeter security include the following:

- Alarm ground level doors and windows against opening and breakage.
- Start day and night security patrols.
- Monitor building perimeter and doors with CCTV.
- Install security access systems to prevent other tenants in your building from gaining access to your company's areas.
- Evaluate exterior lighting. Consider tamper-proof fixtures. Position lighting to prevent deep shadows from the building so intruders can be noticed.

Inside the Facility

Once the perimeter is secured, the security supervisor must often consider how people are controlled in the facility. One effective method is to have all employees and visitors enter the facility through one entry point, with deliveries arriving at another. Photo ID cards should be worn by all employees and visitors should be logged in and escorted by a company employee. Additional measures can include the following:

- Use reception points with properly trained personnel.
- Avoid using stairs as a means of entering and exiting the office environment.
- Use an access control system.
- Provide room and building keys to only those who need them.

- Clearly and permanently mark computer equipment with your company's identification. This will help deter theft and assist in recovering the asset.
- Make the police and any local pawn shops aware of any specific markings on your equipment.
- Keep portable equipment, such as laptop computers, out of sight in locked desks, automobiles, closets, etc. when not in use.
- Increase employee awareness of the threat of theft and advise them of the need to be alert to the activities of people who do not work in their building or area.
- Store recently delivered assets in a secure location until they are set up.
- Staff computer labs when in use and lock them at other times.

Policies

Sound physical security practices must be supplemented with realistic, enforceable asset control policies. For instance, with the popularity of notebook computers and similar items, the removal of such company-owned property should be documented and approved with a property removal pass signed by an authorized manager.

In other cases, a "screening" policy might be considered. This entails making sure only authorized company assets depart the property. It usually entails the inspection of hand-carried items as people leave the facility with the goal of stopping assets from simply "walking out the door." Although the technology becomes smaller each year, and thus easier to conceal, "screening" may still be effective as a deterrent to many potential thieves.

All supervisors, managers, and human resource professionals can also contribute to a more secure environment by supporting sound, time-proven employment policies. This means practicing due diligence when making hiring decisions. Have individual backgrounds and work histories been verified prior to hiring an employee? Has someone checked for criminal records? In short, are the people working in your facility really who they say they are? Although the security supervisor may have little influence over such policies, she must always be aware of the "insider threat." In fact, in many cases, thieves from outside the organization are much less likely than the potential problems originating within your own walls.

Finally, all employees must be aware of their responsibilities as they apply to company-owned property. By holding individuals accountable for company-issued equipment, increased security is usually realized. People tend to be more careful if they realize a lost asset will come out of their paycheck.

Security Devices

In addition to effective organizational policies, there are various technological solutions that can help minimize the threat of high-technology theft. For example, there are many different locking devices on the market that physically secure the asset to a desk or table. In some cases, these devices will transmit an alarm on tampering.

More complicated approach es can include encryption software that encode data stored by a device. This makes the information useless should the device fall into the wrong hands. Similarly, various biometric technologies are becoming increasingly popular in the protection of high-technology assets. For instance, a computer will grant access to a user only after an authorized fingerprint is provided to the system.

The increasing use of radio frequency identification (RFID) tags to electronically track resources has significant potential for securing and managing company property.

There are also various software packages that will discretely "dial out" from a reportedly stolen computer. For example, if a thief attempts to use a stolen computer, a report will be secretly sent out over the Internet to the victimized company—or even the authorities. The report will provide the last known location of the stolen computer so that company security or law enforcement can respond and hopefully recover the asset.

The exact mix of countermeasures and protective policies will vary with each situation. As with other aspects of security, the most effective approach will include a layered approach to the protection of assets. No one safeguard should be expected to provide total security.

Conclusion

Technology in the workplace is a double-edged sword. It allows us to achieve business goals and serve customers. It provides efficient communication and assists in complex management decisions. It does all this and much, much more. However, the presence of high-technology also means increased security threats. Thieves motivated by quick cash, proprietary information, or identity theft can seriously impact your organization. An awareness of such threats and a proactive philosophy can assist the modern supervisor in meeting the challenges of the future.

High-Technology Theft

Quiz

1. Identity theft and the loss of proprietary information can result if high-technology assets are not properly protected. ☐ T ☐ F

2. Trends in high-technology that can contribute to security risks include all of the following, *except*
   A) Smaller sizes
   B) Decreased storage capacities
   C) Increasing convertibility
   D) Growing prevalence

3. The most effective protection plan includes
   A) A segmented approach
   B) A high-technology approach
   C) Sophisticated biometrics
   D) A layered approach

4. A lost asset can result in
   A) Increased insurance premiums
   B) Lost business
   C) Damaged reputation
   D) All of the above

5. High-technology products are increasingly convertible. This means that
   A) They can quickly and easily be turned into cash
   B) They are multipurpose
   C) They can be easily concealed
   D) Their value is dependent on their warranty

6. High-technology thieves can be motivated by
   A) The potential for identity theft
   B) Valuable proprietary information
   C) The promise of quick cash
   D) All of the above

7. The Internet is often used to convert stolen technology assets into cash. ☐ T ☐ F

8. This technology uses electronic tags to help manage and track assets:

   _____

   (Radio Frequency Identification) RFID

9. Effective preemployment background checks can be effective in minimizing workplace theft. ☐ T ☐ F

10. In almost all cases, security threats are presented by outsiders. Employees generally pose little in the way of security risks. ☐ T ☐ F

This page intentionally left blank

5 Designing Operations Control Centers

Colin Best

The concept of centralizing security technology into one control area is not exactly a new concept. As technology evolves, we have to evolve in the way we plan our workspace to house, power, and connect new technologies. In designing and building these centers, we must also acknowledge that these operations control centers are not just the nerve center of technology but also a workspace with a human element. There are many challenges to designing the control center workspace as it is not just an office but a space where humans and technology meet.

Early images of the control center concept were visually represented to the public on television in both science fiction shows and events such as the space program. In the security industry, technology progressed in the form of closed circuit television, recording systems, computerized alarm, and card access monitoring, telecommunication systems to just name a few. In larger, more complex facilities and groups of facilities, it became practical to centralize all of these systems in one location in the form of an operations control center.

This chapter will explain the process of planning and managing the construction of the security operations control center as it pertains to the business it is to be designed for.

Threat and Risk Analysis

As well as being the foundation for a security master plan, the step of preparing a threat and risk analysis is fundamental in the planning process of building the security operations control center. A properly commissioned threat and risk analysis will impact such items such as the control center's location and size. It will likely influence how the control center is equipped and what role will the facility play in the business continuity plan as well as a continuity plan of its own, should the control center facility become unusable either temporarily or on a long-term basis.

Once the operations center is completely built, it will resemble, and be in essence, a data center. The room will house massive amounts of data linked to some mission-critical devices, so the threat and risk analysis will also determine necessary physical security as well as fire preaction and suppression systems, redundant power systems, and backup air conditioning.

The analysis, while addressing the needs of protecting the control center, must also take into consideration the needs of ongoing operations of the facility or groups of facilities being serviced from the centralized location. Accessibility by the facility occupants may be a priority, so the design of the facility should be a balance of the protection of the facility while addressing the needs of ongoing operations.

Feasibility Study

In order to make an educated decision on location of the facility, on completion of the threat and risk analysis, there will likely be several options for the location of the control center. All the options should be examined using a *Force Field Analysis* (Table 5.1). This is a critical

Table 5.1 Force Field Analysis

Force Field Analysis					
Location A		**Location B**		**Location C**	
Driving Forces	**Restraining Forces**	**Driving Forces**	**Restraining Forces**	**Driving Forces**	**Restraining Forces**
Ease of access from main loading dock	Cost of structural change	Ease of access from main loading dock	Cost of electrical infrastructure	Easily reusable space. No significant change to structure	Access from loading dock area not convenient
Accessible to employees and contractors	Proximity to diesel storage	Easily reusable space. No significant change to structure	Not as easily accessible to contractors and employees as locations A and C	Secure and protected	Cost of electrical infrastructure
	Impacts access to loading dock area	Secure and protected		Accessible to employees and contractors	

part of the planning process and should involve internal input from operations management, security management as well as the five construction design disciplines of mechanical, electrical, architectural, structural engineers, and interior designers. Retaining a security consultant to coordinate all the construction and design disciplines would be a wise decision.

Another significant item to be examined at this point will be the measurement of workload to determine staffing. Usually, a major function of the operations or control center is one of a communications center. Part of the study must examine the volume of telephone calls, intercom calls, and radio calls the center will receive. One of the most significant functions of the control center will be the monitoring of closed circuit television. There have been studies supporting that a threshold of what amount of cameras and for how long they can effectively be monitored at one time by one person. To effectively set up a CCTV system for the best possible monitoring, one should first establish the intent of the camera installed.

Monitored cameras: These are cameras that are the highest priority for monitoring. They may or may not be used for identification during playback but are rather to provoke a response from the monitoring station under certain events. These cameras must be visible to the control center operator as much as possible.

Access control by visual identity: These cameras are typically mounted at entryways with intercoms such as doors and gates to confirm an identity prior to allowing access via remote activation. These cameras usually do not require constant monitoring and can be removed from view of the operator but can be called upon easily to confirm identification.

After the fact video review recording: This description can apply to the two categories above, but if a camera does not meet either of the above categories, it will naturally fall under the category of "after the fact" video review. A camera that has little or no value of monitoring and is not typically called upon to confirm identity likely does not require any constant monitoring. With this, one must examine camera locations of this kind and consider whether there is an expectation by a person in view of the camera that the camera is indeed monitored. Individuals may consider legal action if harm were brought on them in view of a camera that they believed was being monitored. One standard for CCTV installation of valuable reference is the Canadian Standards Council (ULC-S317-96) "Standard for Installation and Classification of Closed Circuit Video Equipment (CCVE) Systems for Institutional and Commercial Security Applications."

In addition to the CCTV monitoring affect on workload, the amount of alarms that are received by the operations center will also help determine staffing and design. In the year 2005, Brookfield Properties Corporation's Calgary offices performed a study and launched an initiative to reduce the number of alarms generated by their card access and alarm monitoring systems. After significantly reducing the number of alarms generated by these systems by ramping up maintenance, it was still apparent that the number of alarms still being realized was unreasonable. The major cause of the remaining nuisance alarms was found to be caused more by human behavior and the need for better key control rather than by any physical malfunction. The company is now instituting standards for installations geared at preventing staff from propping and holding open doors by installing delayed closing piezo buzzers at the door locations. Also, examining key control and retrieving keys that access reader overridden doors was paramount in not only reducing alarms but also strengthening the validity of the card access system's audit trail.

The preferred outcome of the feasibility study will demonstrate the best location and size proposal based on protection of the facility or groups of facilities as well as serving the operational needs of the company. Conclusively, the feasibility study will address the location, size, and function of the control center facility as well as a proposed budget for the design of the room. Typically, the design costs will equal roughly 5 to 10% of the actual construction costs or possibly higher. Additionally, the study will address the equipment needs and recommendations for the actual operational items such as telecommunications, CCTV, card access, and any other necessary equipment.

Design

The determining factor in how to begin the process of design is governed by the decision to build the control center within an existing facility or to build a stand-alone facility from the ground up. Should the control center be built in a stand-alone structure, the process begins with the architectural design. In most cases, the control center will be built in an existing structure or a structure being built by others. In this case, the interior design discipline will be responsible for coordinating the mechanical, electrical, and structural design disciplines in achieving a complete design to the specifications of the feasibility study. The interior design discipline is often incorrectly stereotyped as a function to pick colors and décor and this could not be further from the truth. A qualified interior designer is well versed in the complexities of designing a space that not only stands the test of time in terms of trends but also takes into consideration the operation and maintenance of the space. Components as simple as lighting types are an important part of designing the control center. Usually, an operations control center is a 24-hour, 7 days a week operation, which is subject to more than four times the wear and tear of a typical office space. There are also studies that indicate that the amount and type of light a worker is exposed to when working shift work affects the worker's physical and mental health. There are beliefs that strategically designed lighting may help prevent illnesses such as seasonal affective disorder as well as other afflictions. Lighting frequency or temperature is measured in Kelvin units. Warm white fluorescent light will radiate approximately 3,000 K. Some studies claim that absence due to illness was improved in environments lit with fluorescent lamps emitting light at a frequency of 5,000 K or more. Similar studies claim that light intensity also contributes to worker health. Intensity is measured in foot candles or LUX and can be specified at the design phase. Specialized lighting may also be favored to reduce eye strain due to glare. Also, a well-designed ergonomic workspace could help prevent worker absence due to repetitive strain injuries, or RSIs as they are commonly known. Specifying proper functioning premium grade furniture will pay dividends in lowered replacement cycles and possibly even worker absence due to illness.

The operations center should be designed to accommodate equipment using the EIA310-D standard. This refers to the mounting of equipment in a 19″-wide rack and has become the standard for industrial electronic equipment mounting. Main host computers used to operate CCTV, card access, and telecommunications should be mountable in this format and secured to prevent accidental or intentional damage and/or power loss. Most electronic security systems such as digital video recorders, audio recording systems, and video matrix switchers are

manufactured to this standard. Vertical height of equipment using this format is commonly measured in U, which is short for Units. One U is approximately 1.75 in. in height. Equipment of this standard will have specifications regarding how many Us the equipment occupies; for instance, a digital video recorder server may occupy 4 U of rack space.

In most circumstances, the designer will choose that modular console units be installed to house all the equipment. In this case, usually these modular consoles are built to accommodate equipment mounting with the 19″ standard.

Mechanical

The mechanical designer is typically responsible for the design of the heating, ventilation, and air conditioning systems as well as the design of the sprinkler systems and any other plumbing. Because of the nature and volume of equipment being installed in the space, the mechanical designer may specify that a down firing stand-alone air conditioning unit be mounted on a raised floor to provide adequate cooling of computers, etc.

Electrical

Electrical consultants are key people as they will have to specify a higher amount of service to power all the required equipment as well as design UPS (uninterruptible power) systems and provide access to emergency backup power in the event of a service failure or interruption. They are also responsible for the design of telecommunications wiring and fiber optics for telephone and networking.

Structural

The structural consultant will certify that the space meets the standards of the feasibility study with regard to resistance to explosion and ability of the space to support all the specialized equipment being installed and that any structural changes proposed will not affect the integrity of the structure as a whole.

Tendering Process

Once the space has been designed, an independent security consultant should be able to draft a budget for completion of the project. It is considered good practice to tender the construction of the control center. Publicly traded companies and government agencies will likely have policies regarding fairly tendering jobs of this magnitude. The proper construction of the project by the successful bidders will depend on the completeness and accuracy of the bid documents. Generally, a qualified security consultant can assist or even spearhead this process. The process will begin with the preparation of one or more Requests for Proposal (RFP), Requests for Quotations (RFQ), and other similar documents. The intent of the preparation of bid documents is to help define a *Scope of Work*. In the tendering process, contractors will be cognizant of the competition among their industry peers, so it is imperative that the documents be closely scrutinized for "gaps" where a contractor may see the opportunity for savings in construction by supplying or installing inferior components. Once the process is completed, it is common practice to hire a general contractor to coordinate all the potentially dozens of trades necessary to complete construction. The general contractor will usually aid in reviewing the bid documents prior to issue to invited bidders and will often have valuable input in choosing the successful bids.

Under most circumstances, the successful bidder is the lowest bidder. Justifying the award of a contract to a higher bidding contractor is often a difficult sell to management, as ultimately, they represent shareholders or, in some cases, the electorate. This underscores the importance of the accuracy of the bid documents. There are laws in most jurisdictions dictating the process of tendering major contracts. It is important that the entire process is undertaken with impartiality and with as much transparency as possible.

Usually, a specific day and time is set as the closing date for the submission of bid packages. Any early bids submitted prior to the closing date must remain unopened. Once the closing date and time has passed, the bids are to be opened in the presence of the security consultant and the general contractor and examined closely for content. In some circumstances,

a misplaced comma or other minor error can potentially mean a spoiled bid and the bid may have to be rejected.

Once the successful bid packages have been chosen, all the amounts are compiled in a proposed budget for the project. It is important to consider the ongoing operations of the facility when preparing the budget as there may be need for items such as security coverage, temporary hoardings, walkways, and signage. All the proposed budget items are then compiled on a *Budget Cost Summary* (Figure 5.1). Once approved as a budget, it is necessary to procure all the necessary trades to complete the project. Procurement procedures vary from firm to firm, so it is best to have a full understanding of your company's policies regarding procurement prior to executing a contract with any firm.

Prior to construction, it is most likely that the plans completed by all disciplines will have to be submitted to the local municipal government to issue a *Building Permit*. Under most circumstances, construction cannot begin without its issuance. Under most circumstances, the chosen general contractor can pursue the issuance of a permit on your behalf.

Construction

Once the design phase has been completed and all the participating trades have been retained, the construction phase begins. The Project Management Institute model is a proven method for projects of this scope. Prior to executing construction, a *Work Breakdown Summary* should be prepared. A Work Breakdown Summary is a summary of the project broken down into small, individual tasks. Each task is addressed in terms of the time necessary for completion. The tasks are scrutinized as to what task must precede the next and compiled together to identify the duration of the project using *Critical Path Analysis*. The critical path of the most time-consuming tasks that must be followed in chronological order is compiled. Following this process, a proper schedule can be drafted, usually in the form of a *Gantt* chart (Figure 5.2).

Nothing ever goes as planned. These words could not be truer in the case of managing a project such as building your control center. Once construction begins, the unknowns will begin to surface one-by-one. This is where it becomes vital to execute proper *Change Control*. Change control refers to the processes of properly investigating, pricing, and authorizing changes to the *Scope of Work*. Many items will have no monetary effect on the project. The requestor of the

BUDGETTED OPERATING COSTS

Cost Control Summary

Property:	Building A								Date:	
Project:	Control Room								Job #	
Area	1945000								Code	
Description	**Scope**	**Contractor**	**Budgeted**	**Revisions to Budget**	**Committed to Date**	**Less Holdback**	**Total**	**Date**	**Invoice #**	**Cum. Total**
Design										
Electrical	Design	MEC Consulting	$ 2,880.00				$ -			$ -
Mechanical	Design	AEM Mechanical	$ 1,100.00				$ -			$ -
Structural	Design	Bang Structure	$ 1,000.00				$ -			$ -
Interior	Design / Coord	DDL Interior Design	$ 3,000.00				$ -			$ -
Disbursements	As-builts	DDL Interior Design	$ 1,000.00				$ -			$ -
Security	Study	ABC Security Cons.	$ 12,000.00				$ -			$ -
Design Subtotal			**$ 20,980.00**				$ -			$ -
							$ -			$ -
Construction							$ -			$ -
Electrical	Per design scope	Craft Electric	$ 44,000.00			$ -	$ -			$ -
Mechanical	Per design scope	Wilson Mechanical	$ 6,200.00			$ -	$ -			$ -
Structural	Per design scope	Bang Structure	$ 500.00			$ -	$ -			$ -
Interior	Per design scope	Bills Contracting	$ 51,000.00			$ -	$ -			$ -
Equipment	Per design scope	Advanced Electronics	$ 221,000.00			$ -	$ -			$ -
						$ -	$ -			$ -
Construction Subtotal			**$ 322,700.00**				$ -			$ -
							$ -			$ -
Contingency 10%			$ 34,368.00				$ -			$ -
							$ -			$ -
Budget Before Management Fee			**$ 378,048.00**				$ -			$ -
							$ -			$ -
Management Fee	BPL		$ 18,902.40				$ -			$ -
										$ -
Totals			**$ 396,950.40**		$ -	$ -	$ -			$ -
Cost per Square Foot	$ 0.20									

Budget Approved per:

Date:

FIGURE 5.1 Budget Cost Summary.

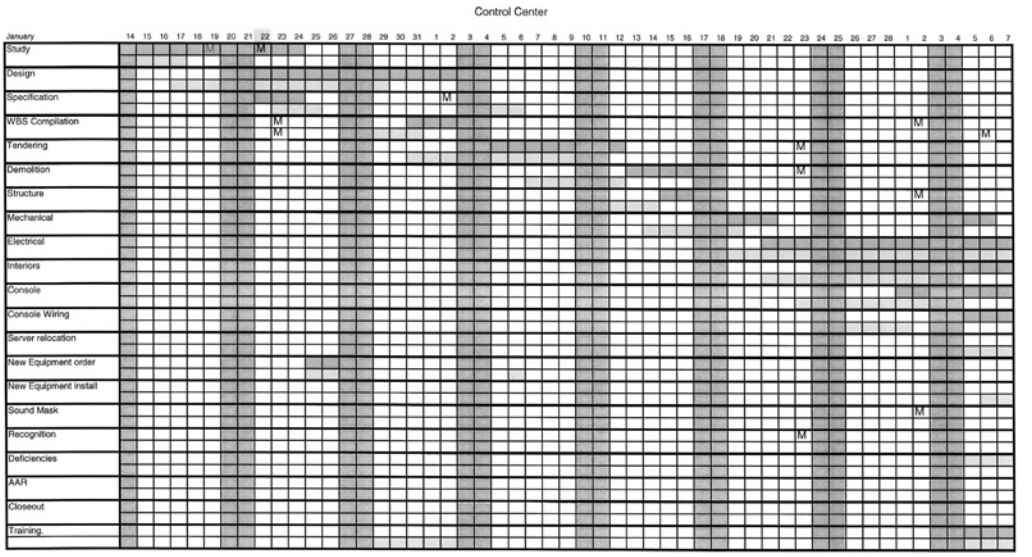


FIGURE 5.2 Gantt Chart Schedule.

change will execute a *Change Proposal*. Once this has been done, the project team will examine the proposal and determine whether the proposed change is necessary and of value. They will also determine what the dollar amount of the proposal is and will ultimately either reject or accept it. If accepted, a *Change Order* or *Site Instruction* will be issued by the appropriate design discipline and issued to the contractor. In some circumstances, a significant change to the design of the operations control center will require approval by the municipality.

As the construction progresses and various changes and site instructions begin to add up, the value of proper record keeping becomes apparent. Hold regular formal meetings and record all items in the form of minutes. Use this forum to discuss progress and schedule as well as change orders and site instructions. Keep copies of all correspondence, meeting minutes, changes, and updated schedules in a project file.

Operational Alignment

As the project progresses to the point of being operational, one of the key steps in successful completion is the proper alignment with operations. Prior to staffing the control center, the proposed staff should have a roadmap of procedures and instructions for properly operating the equipment in the control center. A set of *Standard Operating Procedures* should be developed to provide guidance to the staff working in the control center. While it is anticipated that a complete set of Standard Operating Procedures should be complete prior to staffing, the development of them is an ongoing process as procedures and policies change continuously.

As mentioned in the design process, the protection of data in all the installed systems is a priority and operational procedures should be geared toward the protection of data. Performing frequent routine backups, keeping reasonably sized libraries, and maintaining offsite backup copies will help safeguard data from disaster.

Part of operating the operations control center is the maintenance of as-built documentation. Changes to the room configuration and its connected systems will continue to be a moving target years down the road. As-built documentation should be reviewed at least annually to address changes. Updates should be requested by the appropriate discipline, printed, and filed. As the work area is typically manned 24 hours, special budgetary items should be considered when submitting operating budgets. Cleaning allowances as well as the amounts allocated for regular furniture replacement due to wear and tear should be increased.

FIGURE 5.3 The Completed Project.

Project Closure

The official completion of the project will be dependent on inspections by the security consultant, the interior designer, the municipal inspector, and likely senior management. Once inspection is passed and as-built drawings are prepared, the project finances are finalized and the project is declared closed. The operations control center, shown in Figure 5.3, will be complete.

It is suggested that a postmortem or *After Action Review* be performed as a debrief to the project. This will help determine the success of the project as a whole and not just the physical completion of the operations control center. Important details such as logistics and operational impact are important details that can be improved upon in future projects of this magnitude.

Resources

Canadian Standards Council (ULC-S317-96) "Standard for Installation and Classification of Closed Circuit Video Equipment (CCVE) Systems for Institutional and Commercial Security Applications."

Sources

A Guide to the Project Management Body of Knowledge—(2004)—Project Management Institute (Author and Publisher).

2005 Brookfield Properties Access Systems Alarm Study—(2006, Unpublished)—Brookfield Properties Management Corporation.

Security and Life Safety for the Commercial High-Rise—(2006)—Glen Kitteringham—Publisher: ASIS International.

Review of the Health Effects of Indoor Lighting—(1993)—Steven A. Zilber, B. E.

Contributions

Jolynne Paquette, B.A.I.D—Interior Designer.

This page intentionally left blank

UNIT

VIII

Investigation

This page intentionally left blank

1 Managing Investigations

Robert Metscher

Introduction

Security professionals throughout the security industry are responsible for managing investigations. Whether it is a complex loss investigation, interviewing unwanted visitors or simply taking a report for a customer accident, these are all investigations that require monitoring to ensure completeness. After all, a poorly completed accident report could cost a company a significant amount, should it lead to litigation. It is because of this often concealed responsibility that security supervisors and managers should be capable of adequately managing investigations.

Key Management Skills

Communication

The skill of communication is somewhat vague, particularly in the context of being a manager or a supervisor. Security departments essentially have several different customers, including organizational management, employees, vendors, customers, and any member of the public that may have a legitimate reason to be on the premises. Concise communication is necessary in three separate contexts to lay the foundation for successful information transfer within an organization. First, communication with the security staff or other personnel responsible for submitting documentation cannot be underrated, as it is these individuals that you must count on to accomplish the mission you are supervising. Second, communication with organizational management can be a tricky endeavor often because security must distribute information to more than one department. Finally, communication with organization members, and in this case through committees or when responding to a complaint, can make or break the overall security program. A quick look at these aspects may provide insight as to how they are approached and handled in respect to investigations. Whenever disseminating information to persons or groups outside the security department, it can be helpful to utilize an information dissemination checklist (given at the end of the chapter) to aid in organizing data, clarifying issues involved, and preventing the release of information or sources that could hinder future security operations.

Departmental

Within the security department, information should be shared fairly readily. Even so, there is a certain level of formality that must be maintained. Where that level exists is truly a departmental or organizational matter. Moving information from one shift to another can become a monumental task, which can be overcome with a pass-on book, a simple desk log (see Conclusion), or a formal e-mail process, if operations management software is not available. Oncoming members can verify that a note has been read by initialing the information. Simple desk logs can be useful in reviewing activity levels and officers can also use this as a reference, these logs may be handwritten or a hardcopy printout of the activity stored in an operations database. Memoranda should be reserved for formal communication pertain-

ing mainly to personnel action issues and office policies, while incident information should be contained in the departmental report format or database. Open communications within the department is a key factor in bringing all available investigative resources into use but security professionals must respect the need to compartmentalize some information. A clear example of this occurs when a complaint is made concerning the conduct of a member of the security department, and the manager or supervisor must *investigate* the allegation. This information should be kept confidential and compartmentalized from other members of the security department.

Organizational Management

With respect to investigations in general and internal investigations specifically, this can be extremely sensitive, as managers often want to know "everything" and they want to know it now. If no policy exists, then the security supervisor must come to an agreement with those to whom he or she reports. It is not always prudent to share all current information considering that, should a leak develop within management then a relationship of continuous conflict will evolve. Also, members of management that are not versed in protocols used by a security department can hamper or significantly damage an investigation by demanding specific activities. However, it is also important to coordinate with operations management to compensate for any changes in staffing to due interviews disrupting workflow or suspensions or terminations. It is irresponsible and counter to being a responsible organizational manager to unnecessarily disrupt operations for the sake of the investigations. It will happen when possible communicating with operational managers could avoid the problem. In addition, it is important to act impartially toward management decisions based on investigative conclusions. Investigators seek answers and explanations not convictions or terminations. If an opinion or suggestion is solicited then be forthright and logical, but in any other case your statements should be from a professional standpoint.

Organizational Staff

If there are no current employee committees on security topics, then it may be worthwhile to organize one. It is through this type of involvement and communication with line employees that you as supervisor can get a feel for how security services are *perceived* by one of your customers. Acting on information gained in such meetings will greatly increase the security department's credibility. For it is your department's credibility in providing quality service that will ultimately dictate the level of involvement in security matters by line employees. Put the minutes from these meetings in a monthly bulletin to further increase communication. If you, the supervisor, lack the time or informational content for a purely security bulletin, then consider sharing with a related department such as safety or human resources. Newsletters whether delivered on paper, through e-mail, or as a link to an internal web page are a powerful tool, but technology is creating more robust options. Blogs (weblogs) may be used internally to offer a more timely medium for communication. Why wait for the monthly newsletter when a blog post can be made available everyday, twice, or thrice a week instead? It is also important to remember that same technology can easily link to information on the web, such as articles, white papers, photographs, and video clips, to add some sensational content to the traditional "black on white" paper newsletter. The more line employees that mention the security department's capabilities or consider it a resource, the more likely management will take notice and provide more resources.

Filing Systems

The finest investigation in the world is all for naught if the information is not stored in an easily retrievable and logical manner. Consequently, it is the responsibility of the supervisor and manager to maintain or develop a strong filing system. Such a system must make accommodations for documents dealing with a wide variety of subject matter as well as various access levels. Even computer-based filing of any kind, be they formal databases, spreadsheets, or reports in specific computer directories or folders, there are a few considerations to keep in mind.

Incident/Activity Numbering Practices

Numbering systems associated with cases, incidents, or activity reports can be a deciding factor in the quality of a filing system. Creativity is the key that allows a numbering system to provide quick reference information while remaining uncomplicated. While the most simplistic system would be to just number incidents from 1 to 9,999 little information about the activity involved can be ascertained without physically searching the file. On the other hand, by using just the names of those involved as a means for sorting can raise issues of privacy and may cause complications for multiple incidents or similar names. A numbering system that contains some portion of the activities' date, location, type of incident/investigation, and a counting sequence can provide easy reference. With the increase in the use of computer reporting and storage systems, such numbers can allow for the sorting of databases to measure the levels of various types of occurrences.

2007-0102-4-2-123

The above style of number could represent an event occurring on January 2, 2007 (2007-0102) at a specific location or zone (4), and was a customer accident (2), which by a simple count was the 123 event that year. Such numbering systems provide a great deal of flexibility that can be directly translated into a tracking tool for both activity monitoring, focusing audit efforts and lead development within investigations. Moreover, for larger case files it is perfectly feasible to have a master incident number such as the one above and further assign an additional dash number (–1, –2, etc.) for each document within the case or file. This extra effort can be of great use, should any information within the case file need to be specifically referenced in a later report. Furthermore, categories need not be limited to just 10 options per digit since letters may be used as well giving each digit a total of 36 potential categories of data. Also, by separating each segment of the incident number into individual spreadsheet cells or database fields, it becomes considerably easier to develop management reports by whatever data may be recorded.

Card Support Filing Systems

When an electronic database is unavailable, index cards can become a most valued tool in furthering investigations or just saving time while compiling information with just a little extra effort. For organizations not fortunate enough to have a computer reporting database or one not configured to sort necessary information, card filing systems can take the place of the machine without too much effort. The card filing system can be as complicated as is necessary, allowing key pieces of information from different activities to be sorted in an easily retrievable fashion. Some specific types of cards and their uses are (see also Conclusion):

1. Reference Card: This card will often contain general information about the activity that created the case file. Included on this card is a reference number, which could be the master incident number or a separately generated sequence, and lists the documents that are associated with the case file as well as any other types of cards that have been filed. The reference card is sorted by reference number and acts as the base for the card file structure.
2. Information Card: An information card is a miniature incident report with key information about the individual involved, located at specific points on the card. By placing information at convenient points on the card, it becomes possible to "flip-through" a stack of cards to locate a specific characteristic such as height, sex, aliases, or associates. While it may not be as easy as creating a database query, it can be of value during future investigations. Sort these cards by the last name of the individual described on the card.
3. Identification Card: These cards contain key information taken from the identification presented by an individual detained, arrested, or interviewed successfully. Placing information in specific locations on the card makes "flip-through" review possible for such facts as the state of presented identification or the type of identification presented. This allows for quick cross-referencing to determine any other incidents in which the individual may have also been involved.

4. License Tag Card: In a retail environment, this can be extremely useful in tracking professional shoplifters and smash-and-grab operators. In a general office setting, this can be incorporated into a parking identification system providing for quick notification of employees whose vehicles need some type of attention (headlights, accidents, vandalism). License cards should be sorted by tag number but can also be sorted by the color of the tag itself (first noticed in most situations).
5. Purge Date Card: This card is of great importance in maintaining a useful card reference system, otherwise the sheer volume of cards will make all but the most meager searches impractical. Keep in mind that the purpose of the card system is to allow for quick cross-referencing of incident information to identify trends, problem persons, or areas. As a result, most cards can be purged within a year of creation; however, extending this can easily be done on a case by case basis. If your facility has a very low volume of activity, it may be possible to maintain several years of cards with little trouble. Whenever cards are purged (and destroyed), this should be noted on the purge card or a document destruction log to include the date, specific documents, and the agent/officer actually destroying the information. With the prevalence of electronic databases and spreadsheets and relatively inexpensive cost of continuous storage, there may be no compelling reason to purge data for several years.

Location of Files

Files should be carefully separated as much as space will allow. This aids in preventing information being accidentally "shared" or shared unnecessarily. Divisions of files can be based on the type of investigation involved, with internal investigations being of the most sensitive and important to protect from unnecessary perusal. Realistically, members of the security staff not directly involved with the investigation do not need full access to internal files. They do however need to know the type of activity the individual was conducting if they are to prevent it in the future. Security managers and supervisors should also carefully restrict access to internal training or personnel files maintained within the department. These are in essence partial mirrors of documents maintained in the human resource department and should be provided the same level of confidentiality.

Some specific types of files that should be separated as much as possible are:

- internal training files
- security department activity tracking forms
- customer accident reports
- employee accident reports
- internal investigation files
- external investigation files
- equipment maintenance records
- exception reports—new and old

Keep in mind that as a manager you are responsible for tracking people, their activity, and activity within the organization in general. It is important to share all the appropriate information with your staff, but to provide the same level of individual privacy as does a human resource department in dealing with security staff personnel records. It can be hard to keep some files locked away from your staff and it can cause some questions to be raised about trust, but these can be addressed from a standpoint of the nature of the information and an employee's expectation of privacy. Remember that your employee's curiosity is an important ingredient in preventing or investigating losses, but as their supervisor you must keep this in check in regards to personnel information.

Personnel Concerns

Assigning Investigators

Investigators are often assigned to investigations merely by being the first to answer the phone or arrive at a scene. Needless to say this is certainly not the optimal method for matching

skills to problems, but it may be the most reasonable under the circumstances. Ideally in an environment with limited manpower, investigators should be equally capable to handle any investigation. This may very well be the case but keep in mind that there can be factors within an investigation that warrant the attention of a person with a specific interest. When an individual is an investigator or dons the investigation "cap," it is their imagination, creativity, and most of all their curiosity that ensures a successful outcome. Consequently, officers that are only concerned with the "what" and not the "why" may not be strong investigators and should be encouraged to be more inquisitive.

In a perfect world a supervisor would have all the resources and a specialized investigator for any situation, but as a general rule this is not the case. Supervisors must be able to remove or add investigators to an investigation without overlooking the impact on those individuals involved. To avoid conflicts resulting from reassigning investigators, supervisors should consider possibilities such as using partnering or specializing/centralizing some activities.

It may be very difficult to maintain partner teams in an environment with normally limited resources, but it is possible for a supervisor to assign a secondary or investigative partner on a case-by-case basis. This allows the flexibility to place skills where they are best suited while avoiding problems caused by removing individuals from an investigation. This can also create an even distribution of extra work should an investigator leave the organization. With a fixed partner team, the termination of one partner leaves that individual's entire caseload on the partner, which could become quite burdensome if these should require court appearances or liaison with outside organizations. For those organizations not equipped with case management software, having investigators maintain an individual case log, it becomes rather easy to redistribute a departing investigators cases. Case logs should be designed to reflect the aspect of investigations that are choke points within your investigative process.

Another option available to supervisors is the designation of longer-term activities to one individual. For instance, if your organization has a problem with vandalism or more specifically "tagging," it may be more efficient to assign one officer to handle all these investigations. This does not mean that other officers cannot conduct the initial inquiry and photograph the evidence, but it does imply that the designated individual should track this activity and conduct liaison with the appropriate outside agencies. This is a useful method for lateral promotions that give senior officers more responsibility and experience. This also assists in developing a complete and standardized reporting system for a particular type of activity.

Motivating/Tracking/Evaluating Investigators

The backbone of a good investigation is not generally exciting high-profile work but rather laborious surveillance and endless document review. This can cause an investigator to cut corners or to become more cursory in their work. An ironhanded supervisor can impede investigations by stifling the necessary initiative within investigators, yet a passive supervisor would indirectly cause investigations to falter or become weaker. Motivational methods can be directly tied to supervisory tracking and evaluation efforts of investigators; however, the supervisor must know each member of their team and what motivates them as individuals. Efforts to motivate the individual separate from the team must be made as is necessary and to strengthen the investigator's tie to the team. Here are some useful tools to encourage, track, and evaluate an investigative team. There are, however, a limitless number of ways to motivate, and a supervisor must use some creativity and sound judgement when developing these efforts.

1. Develop a monthly or quarterly review/counseling program. These need not be long counseling sessions but merely a 15- to 20-min session for each agent at the beginning or end of each month. The supervisor can write a few objectives and points of improvement for the investigator to reach within the month and identify topics that the agent will receive training on in that month. The agent in turn can write concerns or suggestions about the points listed and any comments about the department's operations. This not only provides useful documentation to support an annual review but also gives the individual a feel for their overall performance. For the supervisor this can offer valuable insight into the attitudes

of the department and likely avenues for future motivation and improvement. It should also be noted that supervisors must be prepared to receive some fairly harsh criticism from their staff and that such criticism must be acted on but not retaliated against. If the staff is willing to write their criticism, then they are concerned about their workplace and are not simply "punching the clock." This is positive and can be harnessed.

2. Hold well-defined meetings regularly. Keep these as short as possible by using a standard naming system that helps to identify the purpose. Names such as solution meetings, planning meetings, and organizational affairs meetings can create the right mind-set prior to attendance. Limit the agenda to one or two topics in a meeting and strive to keep these under 30 min in length. Never forget that meetings should ultimately increase productivity and not become a barrier. If necessary, designate an individual to act as a facilitator to prevent the meeting from being sidetracked.
3. Allow the staff some say in general operations. Foster an open environment that encourages suggestions that can streamline operations. Don't be afraid of using some of these ideas. By incorporating everyone's ideas, the staff gains a feeling of ownership of the department, and consequently their interest and concern will increase further.
4. Develop a lessons learned journal. This can consist of a list of all cases with short entries describing the circumstances. Also included are actions that should not be repeated (hence lessons learned) as well as compliments for activities that were handled exceptionally and that agent's name. This provides a lasting acknowledgment of an investigator's achievements.
5. Various charts can be used to show progress and organize activity. Flowcharts (see Conclusion) can be used to graphically guide investigations and as a reminder as to who is responsible for finding different information. Load charts (see Conclusion) can be a quick reference to show the number and length of investigations for which each officer is responsible. The example makes it plain that Smith is dealing with far fewer investigations than his peers are and this can be a tool in motivating Smith. Smith may not realize how much less he is doing and such a graphic representation is undeniable. This can be replaced by a Gant chart if project management software is routinely used. The primary difference is the accuracy of the information as more precise data would typically be entered into project management software.

To help level the work load and to ensure that mundane tasks are not too mundane, internal audit activities can be developed by a supervisor. These audits can be a natural extension of patrol or other activity that aids in enforcing or monitoring protection standards—perhaps monitoring the use of safety equipment by line employees or searching back areas for concealed merchandise.

Investigation Issues

Initiating and Prioritizing Investigations

Investigations are initiated for many reasons and in diverse circumstances; however, the security supervisor is often directly responsible for those generated by exception reports, audits, or unique incidents. These investigations must be prioritized and worked into the department schedule. The security supervisor should seek to have a staff investigator handle much of the so-called "legwork" so as not to cause a slighting of supervisory duties. This in no way implies that the supervisor can simply pass off the work he or she just does not feel like doing, but instead offers training and experience opportunities for other investigators. Supervisors can use all investigations in which they are directly involved as an opportunity to mentor another experienced investigator.

Once an investigation has been initiated, lead sheets, which for practical purposes can be index cards, should be created for each lead that is discovered. These can then be systematically researched or divided up among agents for follow-up. These lead sheets should contain basic information about the investigation (incident number, type of incident, date, etc.) as well as the lead itself. Similar leads can be grouped onto the same sheet, as they

will most likely be researched at the same time. Any information that is discovered from the lead should be briefly noted on the lead sheet since any evidence (receipts, photographs, vouchers, etc.) would most likely be kept separate from the lead sheet itself. Completely researched leads that provide no further leads can then be returned to the primary investigator or the case file, while any further leads can be noted on the original sheet before a new sheet is created and researched. Lead sheets are of unquestionable value when an investigation is paused or stopped, especially if the primary investigator leaves the organization during this time. In addition, this type of documentation allows the supervisor to quickly review investigations to determine the level of effort and effectiveness of an investigator.

Prioritizing investigations should not occupy more than a few minutes of a supervisor's time, but these decisions can have a great effect on the security department, the parent organization, and the public's opinion of the organization. Careful consideration must be given to high-profile incidents or when senior executives are implicated in wrongdoing. Failing to properly judge the amount of emotion behind an investigation or the opinions of organizational staff, management and the public could cause serious embarrassment to the parent organization. Factors for prioritizing investigations include but are not limited too:

- emotionally charged issues (i.e., workplace violence, hate crimes, stalking)
- high-profile incidents (media or prominent figure involved)
- organizational management interest
- total investigative resources available
- total protection obligations
- likeliness that activity investigated will cease quickly
- number and quality of leads
- solvability factors considered and reviewed:
  - Was there a witness?
  - Can the suspect be:
    Named
    Located
    Described
    Otherwise identified
- Can a suspect vehicle be identified?
- Is stolen property traceable?
- Is a clear suspect MO present?
- Is there significant physical evidence present?
- Is there a positive report concerning physical evidence by a trained technician?
- Is it reasonable to conclude that the case may be solved by normal effort?
- Was there clearly limited opportunity for anyone but the suspect to have committed the crime?

Investigative priority is a frequently changing situation with investigations being set aside for periods of time when necessary. A word of caution goes with this and that is to avoid unnecessary shuffling of investigations. If an investigation is nearly complete, there is little reason to drop it simply because of an artificial priority system.

Investigative Follow-Up

The security supervisor is directly responsible for ensuring the completeness of case files and all documentation included within, and therefore must take several actions during and after an investigation. The supervisor must monitor progress, coach investigators, and be prepared to summarize the investigation to management on its completion. This is a tall order but is essential to building departmental credibility with organizational management and outside agencies.

As discussed previously, progress reporting can occur in several different ways as well as being an inherent part of the coaching process. It is important to identify an investigator's improper actions as quickly as possible to prevent them from occurring again and to recognize proper actions in an equally timely fashion. One coaching method includes three steps on identifying the incorrect action. First, a positive activity is recognized and encouraged, followed by the incorrect actions being verbalized to the individual and the correct way explained or

demonstrated. The positive reinforcement can be placed at the end but it illustrates one way to correct behavior while avoiding an unconcerned presentation of the supervisor's interest. As the investigator is coached through the investigation, the progress can be easily monitored. It is with more experienced investigators who may not seek assistance often that progress must be monitored through other techniques.

Another extremely important tool for coaching investigators is to play "devil's advocate." So long as the investigators know that you are not attacking them personally or questioning their character in a real sense, this can be very useful and often quite fun. Simply question all aspects of the investigator's report and try to put yourself in the shoes of a defense attorney. By attempting to find holes in the report or case and picking at them, it becomes possible to search for other information and aid the investigator in remembering the important aspects of the investigation. At the right time, this can be very enjoyable for all involved and is also useful in offering newer investigators a feel for questions they may be confronted with in the future. The operating terms here are informal and impersonal. In all ways prevent the investigators from feeling that their peers are personally attacking them.

In addition to ensuring that parts of a case file are complete, take the time to make sure the case file contains all the appropriate parts. Develop checklists that aid in keeping files complete from start to finish. Checklists should seek to eliminate relevant problems through prevention rather than merely identifying the existence of a problem after the fact. For example, begin with the completeness of the prepared case file to ensure that all necessary forms are present at the start, which also serves as a reminder of the requirements of the various parts of the case file. Again, try to keep paperwork to a minimum, as it should contribute to the overall productivity rather than creating extraneous work. When using an electronic database for reporting many of these, actions and requirements may be automated.

Once the investigator has completed the case file, the supervisor can write a summary of the case in the lessons learned journal. Later, this can be used as an executive summary in memos forwarded to organizational management. The summary should be extremely brief, identifying unique aspects of the case as well as actions taken, and the current disposition. Below is an example of such a summary:

Review of alarm access reports identified access activity at the satellite location outside of normal business hours. Subsequent surveillance and investigation identified a total of approximately $5,000 in potential loss through property theft, and identified newly hired manager John Smith's code as the one used for access. During the interview, Smith admitted to the theft of property totaling $5,000 from the satellite location as well as $2,300 in fraudulent invoices for undelivered services. Smith agreed to pay restitution in full and criminal charges have been filed. Total loss in this case is approximately $7,300 and a new exception report has been developed to aid in a more timely identification of similar loss opportunities.

After the case file is completed, the supervisor must review further aspects of the case, such as evidence preservation, and conduct one last review of all the paperwork. Proper preservation of evidence can prevent uncomfortable courtroom situations. The local prosecutor's office should be contacted and preservation practices reviewed. Any time evidence may be maintained outside of a police evidence operation, it is likely that some questions will be raised about chain of custody and access. A little extra time spent on this matter may lend considerable credibility to one's department in the future. Moreover, it is important for the supervisor to review all cases with investigators prior to their court appearances. The investigators should do the same for the supervisor on the days of his or her appearances. The fact that court appearances can occur months or even years after an investigation is completed makes this review and drilling of great importance. This is just another application of the old adage, "… a gallon of sweat in training is better than a pint of blood in battle." Keep this in mind when an investigator grumbles about the extra effort.

Information/Intelligence

Investigative supervisors are expected to have volumes of current information literally at their fingertips at any given time. They need to have a firm understanding of local and regional trends that could affect their organization. Collecting and maintaining information can be a very useful tool with little extra effort in the long run. Using a card filing system like the one mentioned earlier, it is possible to track activity in the vicinity of the organization, which

quite possibly becomes the source of a lead in a later incident. When using an electronic database trend reporting capabilities are considerably easier than with paper-based intelligence. Intelligence analysis software such as Analysts' Notebook by I2 (www.I2.com) offers powerful tools for correlating data quickly.

Information can be located from a variety of open sources such as newspapers, phone books, crisscross directories, and the World Wide Web. Newspapers often have a section on police-reported incidents in the area. This can be of tremendous value in recognizing activity trends in the immediate area. When one is at a court appearance, it only makes sense to listen to the other cases being heard and if any are for activities related to your organization, then make note of this. It is possible that a robbery could occur in a mall parking lot while the tenant stores remained unaware of this activity. If your organization were located in or around the area, this information might be useful in determining staffing needs and informing employees. As with any information collection and storage function, it is important to regularly purge the records to maintain just those that will be useful.

Any information provided by an individual, whether solicited or not, must be carefully reviewed to determine credibility. The following questions represent the minimum scrutiny such provided information should receive.

Why did this event happen?

- At this particular time?
- At this location?
- Why is this information being provided to us?
- Presented in this fashion with this slant?
- Why does or doesn't this information stand up when compared to all other information available?
- Why or how will someone or some group benefit by others believing this information?

Always keep in mind that information that is received or developed may be false or incorrectly organized. This may be intentional or not; however, the result is the same. Investigators must seek to corroborate any information to ensure its accuracy.

Conclusion

Nearly all security supervisors are responsible for managing investigations of one type or another. An accident investigation in one organization may be as important as a theft investigation is to another organization. It is the supervisor's responsibility to ensure that investigations are complete, accurate, timely, and meet the needs of the organization. Minutes spent preparing can save hours in unnecessary effort. Supervisors need to create strong investigation support measures such as filing, mentoring, and information storage to provide the greatest long-term value from the investigative process.

Information Dissemination Checklist

1. Check existing notes
2. Update facts and data
   a. Identify information that, if leaked, would be detrimental to the intended security department activity and remove mention of as much as possible.
3. Consult with other staff (other departments as appropriate)
4. Identify target audience
5. Primary—that is, *vice president of operations*
6. Secondary—that is, *CEO or president and all other vice presidents*

Prepare key messages (i.e.)

   a. *This activity directly affects operational efficiency.*
   b. *This activity impacts on profitability.*
   c. *This activity impacts on morale.*

   d. *This activity can be largely prevented.*
   e. *Our suggestions are necessary to effectively prevent negative impacts of this activity.*
7. Develop positioning statement
8. Develop theme
9. List example or analogy
10. Provide quotes
    a. Sound or video bites
    b. Excerpts from reports and written statements
11. Role play potential questions and answers

DAILY ACTIVITIES LOG DATE _____

DAY _____

OPENING CLOSING

_____ FITTING ROOMS _____ FILE AUDITS

_____ MAIL _____ CLEAN OFFICE

_____ CLEAN INTERVIEW ROOM _____ CHECK DOORS

DAILY AUDIT EXCEPTIONS: LP SCHEDULE

NAME HOURS

_____ **REGISTER AUDIT:** REG# _____ RESULT _____ _____

SEARCH _____ _____

_____ **REGISTER AUDIT:** REG# _____ RESULT _____ _____

SEARCH _____ _____

_____ **REGISTER AUDIT:** REG# _____ RESULT _____ _____

SEARCH _____ **EXECUTIVES**

NAME HOURS

_____ **INKTAG COMPLIANCE:** SECTION _____ #UNTAGGED _____ _____

RESULT _____ _____

_____ **HOLDS COMPLIANCE:** RESULTS _____ _____

TIME INCIDENT/DESCRIPTION/ACTION TAKEN/BY

CASE NUMBER CASE NAME RESULTS WHOM

REFERENCE CARD PURGE DATE CARD

Ref# Type Ref# open MM/YY

Last Name First Name MI MM/YY of Scheduled Purge

Aliases: Note extensions

DL# State

TAG# Color Make Model Total Documents: #Purged:

Documents:_____ Purging Agent:

1 Witness

2 Witness

3 AGENT Doc# AGENT

INFORMATION CARD LICENSE TAG CARD

Last Name Ref# Type TAG# State REF# Type

First Name Middle Sex Race

Address: Ht Wt Color Make Model Year

City ST Zip DOB/Age

Phone# ID'ing information

Aliases: Associates:

Details of information

Doc# *details on back* AGENT Doc# AGENT

IDENTIFICATION CARD

ID# State REF# Type

EXP

Last Name First Name MI

Address

City ST Zip

Phone

Doc# AGENT

Investigations

Quiz

1. It is important to act impartial to management decisions based upon investigations. ☐ T ☐ F
2. An extremely important tool for coaching investigators is to play _____.
3. Managing investigations is the responsibility of the:
   a) Security director
   b) Team leader
   c) Human resource department
   d) Security supervisor
4. Three examples of information cards are _____, _____, and _____.
5. Factors for prioritizing investigations include but are not limited to:
   a) Organizational management interest
   b) Total protection obligations
   c) Number and quality of leads
   d) All of the above
6. Gathering information is the primary role of the investigator. It is not necessary that the investigator seeks to corroborate any information to ensure its accuracy. ☐ T ☐ F
7. One of the most valued tools in furthering investigations is:
   a) Binoculars
   b) Tape recorder
   c) Index card filing system
   d) None of the above
8. To avoid conflicts resulting from reassigning investigators, supervisors should consider possibilities such as using partnering or specializing or centralizing some activities. ☐ T ☐ F
9. _____ and _____ are expected to have volumes of current information literally at their fingertips at any given time.
10. Failing to properly judge the amount of emotion behind an investigation or the opinions of organizational staff, management and the public could cause serious embarrassment to the parent organization. ☐ T ☐ F

2

Developing Report Writing Ability in Subordinates

Christopher A. Hertig

If one were to query most security supervisors about the most pressing problems they have with their subordinates, there is an excellent chance that the reply would be:

Poorly written reports.

Report writing is a *process*. It consists of obtaining information—usually through interviewing—making notes on it, and organizing it into a readable, useful format. Whichever format is used, the essential elements are the same. Unfortunately, professional report writing is difficult. Many people have never been taught how to do it; some lack the literacy skills necessary and others simply don't want to do it. All of these obstruct the process and create problems for supervisors.

In assessing report writing competency, the supervisor should be on the lookout for these problem behaviors:

- *Avoiding writing the reports*. This can take the form of delaying and procrastinating as much as possible the writing of the report. It can also manifest itself in avoidance of incidents that would give rise to having to write a report. Some of these officers become "World Class Avoiders" and seemingly never have incidents or conditions of concern on their shifts. Others invariably arrive late at the scene of incidents.
- *Failing to log or note all pertinent conditions*. This may be simple laziness or the emulation of an inappropriate role model. It may also stem from the officer not realizing the importance of complete documentation. A few questions to ask in regards to diagnosing this problem are:
  1. Who reads the reports?
  2. How is feedback on reports given to the officers?
  3. Are officers educated—not merely told—of how the reports will be used by insurance carriers, accreditation agencies, or courts?
- *Failing to proofread the report*. This is probably the most common mistake for we are our own worst editors. Few of us can adequately critique our writing effectively. Some methods of overcoming this are:
  1. To have a fellow protection officer review the report.
  2. To provide immediate and constant supervisory review so that every report gets scrutinized—pounce on the reports!
  3. To have officers sign the reports so that they feel a sense of formality and commitment to their work product.
- *Inadequate detail/descriptions*. Have them make rough sketches. Also consider making or using existing codes for areas of the facility and proximity to subjects (#2 Position, etc.).

- *Inadequate command of the English language*. Educational levels must be increased! The role of the protection officer must be fully understood and appreciated in terms of the communication aspects of the position. Job descriptions must make mention of this and hiring practices must reflect it.
- *The demeaning of officers who write well by other officers*. This does not occur in all workplaces, but it can easily take root if supervisors don't manage the employee socialization process effectively. When one hears comments such as: "*OK, here we go again 'Dark and Stormy Night' is gonna write another report*"; the obvious inference is that negative, counterproductive forces are at play. This cannot be tolerated. Supervisors must take every opportunity to advance and advocate for higher education, increased training, and greater professionalism within the protection organization.
- *Lecturing or complaining by supervisors about inadequate reports when practice sessions in report writing have not been given!* This is a problem *owned and controlled* by the supervisor. He or she must give practice in writing in order for the skill to develop. Along with this practice—usually preceding it—is the presentation of a model behavior. Show "The Troops" a well-written report.

Writing Across the Curriculum

Colleges have taken the position that students do not learn to write in English composition courses, rather they learn to write by applying the basics of writing learned in English composition in other courses. They write in various writing intensive courses.

Note taking—notes are the foundation of the report. A simple way of remembering this is the equation:

NO NOTES = NO REPORT

Note taking can be and should be taught throughout any instructional process. The most casual review of class participants will usually reveal those with college and those without as the college educated take notes. They have learned not to trust their memories. More importantly, they have learned to take notes on information in an organized, retrievable manner.

One technique for teaching writing is to have class members read each other's notes. In this way they can share perspectives, are on notice that they must be active participants, and get practice in this crucial skill. Having them take notes in "bullet" format with some space between each line is a good practice. This leads in to writing reports—and memos—in a "bullet" format. This format is accepted in business circles and easier on both the writer and reader.

Perhaps most important in having class members read each other's notes is that it moves them toward that most difficult roles: editor!

Interviewing—without conducting an effective interview, there will be no useful information to make notes on. As most information comes from people, interviewing is a critical investigative skill.

Violence management—the documentation phase of the violent event. Obviously any use of force must be documented completely. Note that encounters don't have to be physically violent in order to require thorough and complete documentation; simply enforcing a rule, evicting someone from the property, or taking away a privilege all call for complete documentation. All are situations where the officer's actions and judgement will be called into question.

Crime/Incident scenes—similar to violence management, the protection officer's observations and actions need to be documented at the scene of all crimes and incidents. Short note taking and report writing practice sessions can be meshed in with instructional sessions on crime/incident scene management. In instances where doing an actual writing practice is not practical, it is good practice to review verbally the items that must be noted. In this way, students can develop "an eye for documentation."

Testifying—testifying in legal (criminal or civil court) or quasilegal (disciplinary hearings, administrative agency hearings, labor arbitration hearings) proceedings is the final product, the epitome of an investigation. There are some who believe that testimony starts with the taking of notes. One could probably argue that it starts earlier, with the interview or initial approach to the incident under review.

Whichever is the case, testimony is the presentation of an investigation. It is where the officer shows his or her work on the case. It is also, like report writing, an exercise in communication.

When teaching testifying, it is relatively easy to tie in report writing; one needs only to challenge or attack the report that was written by a student. Challenges to the descriptions of persons and objects drive home the import of attention to detail. Questions about the officer's sources of information illustrate the criticality of attributing everything learned to its proper source. Queries regarding the definitions of words in the report emphasize the need to use simple terms, avoiding technical jargon or "legalese."

Note that there are other benefits to emphasizing testifying, such as improved presentation skills for conducting meetings, enhanced public speaking ability for dealing with crowds, and a better understanding of the legal/quasilegal environment. An astute instructor could use testifying to develop public speaking skills that are normally avoided by adults.

Supervisors must ensure that quality reports are written by *all* protection officers. The supervisor must be a role model *and* a coach in the report writing process.

Developing Report Writing Ability in Subordinates

Quiz

1. If one were to query most security supervisors about the most pressing problems they have with their subordinates, there is an excellent chance that the reply would be poorly written reports. ☐ T ☐ F
2. Report writing is a process that includes (select best answer):
   a) interviewing
   b) making notes
   c) organizing it into a readable, useful format
   d) all of the above
3. Avoiding writing the reports in a timely fashion has no bearing on the overall process. ☐ T ☐ F
4. Proofreading of the report should be left solely to the supervisor on duty. ☐ T ☐ F
5. Note taking is the foundation of the _____.
6. An effective technique in note taking is (select best answer):
   a) always utilize capitals
   b) utilize a shorthand method
   c) utilize bullets
   d) none of the above
7. Without conducting an effective _____ there will be no useful information to make notes on.
8. Nonphysical violent events need not be reported on. ☐ T ☐ F
9. Testimony is the presentation of a _____.
10. The supervisor must be a _____, _____, and a coach in the report writing process.

This page intentionally left blank

3 Testifying in Court

Christopher L. Vail

Testifying in court is like firing your weapon in the line of duty—it's unlikely you'll ever have to do it, but if you do, you'd better be accurate! There is always the possibility that you, as a security supervisor/manager, will have to testify in a court of law. Court appearances can be intimidating and frightening to those who have little or no experience in testifying. This chapter will do more than just alleviate fear of testifying. It will prepare the security supervisor/manager to present his or her testimony in a confident and professional manner.

Grand Jury vs Trial Jury

The grand jury, the initial step in the trial process, decides whether to prosecute based on the strength of the evidence offered by the prosecutor. This evidence may include oral testimony of a security officer. The grand jury environment is ordinarily a relaxed and informal setting in which the prosecutor presents the case to a jury, usually consisting of between 6 and 24 jurors. Grand jury proceedings are conducted in secret and are closed to the defense counsel, press, and the public. Nevertheless, the grand jurors get an immediate impression of the professional training, skills, and abilities of the testifying officer and his or her agency.

Since testimony presented in front of trial (petit) juries is done in open forum, the press and public can closely scrutinize a testifying officer's professional conduct. Testimony should be presented in a confident and professional manner. Trial juries consist of 6 or 12 jurors who consider your testimony, the oral testimony of other witnesses, and physical evidence to decide on the guilt or innocence of the accused.

Expert vs Regular Witness

An expert witness is considered to be one who is qualified to speak with authority by reason of his or her special or unique training, skills, or familiarity with a particular subject. An expert witness is allowed to render opinions and draw conclusions (in contrast, witnesses not qualified as experts are generally not allowed such latitude). A person becomes qualified as an expert witness by demonstrating to the judge, or sometimes the jury, that he or she has the required education, knowledge, training, and/or experience to qualify as an expert in the subject matter under consideration.

Most police and security officers do not qualify as expert witnesses as their duties are usually more general in nature. In most cases, an investigating security officer can testify only to that information of which he or she has personal knowledge. For example, while the case may have involved questioned documents, the officer can only testify as to what he or she knows about the documents and cannot testify as to the authenticity of the documents themselves. The document examiner in the case would be the expert witness.

Preparation for Court

Probably the most important part of being a successful and confident witness in court is your preparation before testifying. The first step in this preparation is to realize that

you may be called on to testify on any official act you perform in your job as a security supervisor/manager. Preparation actually begins at the scene of a crime or when conducting the initial investigation. Officers should consider every call, complaint, and investigation as possible material for a future court case. In every case and in every investigation, think ahead about the possibility of having to testify to all your actions in that particular case. The easiest way to do this is to picture the judge, jury, and/or defense counsel looking over your shoulder as you perform your duties and ask yourself such questions as "How will I explain this on the stand?," "What if they ask me about this?," and "Can I explain this action in court?"

Review your case in detail before going to trial. You may have forgotten just enough to present some inaccurate information and put reasonable doubt in the mind of the jury. If you are going to testify concerning a situation that happened months or even years earlier, you will have to refresh your memory. Refer to the notes you took at the scene of the incident. Review any reports you wrote regarding the incident. Talking with coworkers who may have knowledge of the situation may help you to recall forgotten details. But, do not try to develop a common story. Remember your testimony must state what you recall, not what somebody else told you.

Let's take a quick look at notes as they may be of assistance to you in court. Officers who perform their job professionally are well aware of the necessity to take good field notes, maintain good field notebooks, and prepare well-written and accurate reports in all cases. Field notes and the notebooks in which they are kept represent the basic source of information drawn on when writing the incident, offensive, or investigative report. They are very valuable and of great assistance when the officer testifies in court.

Field notes should begin with the officer's assignment to a case and continue until the case is closed. The time and place to get factual data and information is at the scene during the initial investigation. Anything omitted or overlooked is either lost or must be ascertained later. That is usually a difficult, time-consuming task that often leaves out important facts that may be crucial testimony or evidence in court.

If you pictured the judge, jury, and/or defense counsel watching over your shoulder during the investigation and listening to your interviews, you will find that your notes, which may be introduced as evidence in a trial, and your reports (written from your notes) will be more complete, thorough, and accurate. Your self-confidence will be evident to the judge and jury, and you will actually feel better.

If documents, photographs, records, etc. are going to be introduced into evidence in your case, gain some familiarity with them. You don't need to be an expert, but you should become generally familiar with their use, purpose, and how they are used in the normal course of business.

Look for discrepancies between the field notes and the report and be ready to explain these differences. This comparison between field notes and reports will take place and could destroy your credibility.

Speaking and Acting with Confidence in Court

It is said that an audience remembers 7% of what you say, 38% of how you sound, and 55% of how you look. A jury, like any other audience, is made up of real people. It can and will have feelings about you as a person, not only as a witness. They may like or dislike you, respect and admire you, or look at you as an incompetent idiot. Juries, like other audiences, are not easily deceived. If what the jurors see and hear is believable, they will believe it. You can win their trust, respect, and admiration by appearing confident, self-assured, and by telling the truth. Even before getting into court, there are some things you should do that will assist you in presenting a winning case. Following these guidelines will help you to develop that feeling of self-confidence that can help your case.

1. Know which courtroom you'll be testifying in. If you are unfamiliar with the particular courthouse or courtroom, check it out before the trial so you will appear to know your way around.

2. Know who the major players are: the prosecutor, defense counsel, and judge. Learn something about them if possible; the more you know about them, the more comfortable and confident you'll be.
3. Do not discuss anything about the case in public or where your conversation may be overheard. You just don't know who could be a juror or defense witness!
4. Treat people as if they are the judge, defense counsel, defense witness, or juror in your case going to trial. Your professionalism, politeness, and courtesy will be noted and remembered—especially by those who do see you in court as a witness.
5. Do not discuss your personal life, official business, biases, prejudices, likes and dislikes, or controversial subjects in public for the same reasons above. You might create a poor impression on a judge, juror, defense counsel, or witness.
6. Always be on time for your case. Know what time you will be expected to be called.
7. Dress appropriately at all times. Look businesslike and official. If in uniform, it should be clean, neat, and complete. (If you don't know, check in advance if you need to leave your weapon off.) If not in uniform, a neat and clean sport coat and slacks are as appropriate as a business suit (male and female officers alike).
8. Try to avoid the defense counsel and any defense witnesses before the trial. You should assume that they will try to take advantage of you and get you to say something about the case. If you do say something, look for it to appear later, in a way to discredit you and your testimony.

Now that you have started to develop your self-confidence and are beginning to realize that you can handle testifying, let's discuss how to be even better prepared.

The famous Dale Carnegie way of building self-confidence works extremely well to prepare yourself for doing something that most people fear the most—speaking in public. In the 1977 best seller, *The Book of Lists*, speaking before a group was the number one fear listed in a category called "the fourteen worst human fears" (the fear of death was listed sixth). Fear is the strongest enemy of good communications. It is shown by nervousness, tension, and self-consciousness. After starting his course, Dale Carnegie said: "… little did I realize that this training would prove to be one of the best methods ever yet devised to help people eliminate their fears and feelings of inferiority. I found that learning to speak in public is nature's own method of overcoming self-consciousness and building up courage and self-confidence."

The Carnegie approach to self-confidence is potent medicine for those who, like the 85% of the public (security officers included), dislike or absolutely fear speaking in public. After all, testifying in court is public speaking, isn't it? Even in closed grand jury proceedings, you are speaking before others. The "stomach butterflies," which grow into flailing monsters in many people, don't know the difference between courtroom testifying, grand jury proceedings, or speaking to an audience of hundreds.

A very brief summary of Carnegie's self-confidence development course (see *The Quick and Easy Way to Effective Speaking*, Dale Carnegie, Dale Carnegie & Associates, Inc., 1962) will help you to be a self-confident witness. The basic tenets of this excellent program are:

1. Realize that you are not alone in being afraid to speak in public.
2. A certain amount of stage fright is useful. It is nature's way of preparing us to meet unusual challenges in our environment. Be aware of this and keep those psychological preparations (pulse beating faster, respiration speeding up) within limits. Doing so will make you capable of thinking faster, talking more fluently, and generally speaking with greater intensity than under normal circumstances.
3. Most professional speakers never completely lose all stage fright.
4. The chief cause of your fear is simply that you are unaccustomed to speaking in public. For most people, public speaking is an unfamiliar experience, and therefore, it brings out many anxiety and fear factors. The way to beat this is to practice as much as possible.
5. Be prepared: "Only the prepared speaker deserves to be confident."
6. Preparation does not include memorizing.
7. Predetermine your mind to success; lose yourself in your subject. In law enforcement terms, this means "know your case well." Keep your mind off the negative stimuli

that may upset you, and it is especially important to keep your attention off yourself. Give yourself a "pep talk"; "psych" yourself up.

8. Act confident. Take a deep breath; sit or stand up straight; look your audience straight in the eyes; and talk as confidently as if every one of them owed you money.
9. If you have pr epared yourself all along, you will be more confident.

If you follow and practice the Carnegie method for developing self-confidence, you will be more confident about your testimony in court. You will be able to explain not only what you did (or didn't do) but why you did (or didn't) do it. Many of your answers will have already been prepared at the scene or during the investigation. These principles are tried and true. Go back and read them again, learn them—they do work.

Knowing and practicing effective techniques of public speaking is synonymous with winning; you feel positive, confident, and self-assured. You reflect the presence that says you are strong, determined, persuasive, and in control. The jury will listen to you, you will gain and hold the attention of the jury and you will effectively sell your case and yourself to the jury.

The first step in effective public speaking is to be comfortable. You must appear to be both comfortable and in control. Use erect posture as this suggests authority. If you are standing, your feet should be about shoulder width apart, suggesting solidity and confidence. Your hands should rest comfortably at your side, showing you to be a natural and comfortable person. If you're sitting, lean slightly forward, but do not slump in the chair. Have your hands in a comfortable position and do not play with rings, pencils, your notes, etc.

Overcome your fear of speaking in front of a group by learning how to breathe properly. Proper breathing requires taking deep breaths, but not allowing your shoulders to heave so you look stiff, scared, or intimidated. Deep breaths shouldn't be seen above the rib cage; your lungs need to expand outward, not upward.

Relax by first tightening your muscles, then relaxing them. An easy way to do this is to get out of public view. Do this at home or in a private location before going into court. Take a few deep breaths to clear the air in your lungs, then tighten and relax the muscles in your body a few times. Be careful you don't get a cramp, though.

When testifying, what the jurors see is sometimes more important than what they hear. Your appearance should be neat, clean, and you should show confidence, not cockiness. Your tone, eyes, face, and appearance all send signals; they have the power to make a strong impression that can contribute to whether you win your case.

Be careful when using gestures. Do not cross your arms over your chest. Do not raise your fists or pound the air as if you are making a dictatorial presentation. Use no pointing gestures toward the jury or defense counsel. While you may wipe the sweat off your brow occasionally, do not let it indicate nervousness. Don't show signs of nervousness such as playing with rings on your fingers, pencils, notebooks, and frequent crossing and uncrossing of your legs.

Use your voice to your advantage. The presentation should be loud enough to be heard by the juror furthest from you. But use a natural voice, only speaking with the volume needed to be heard clearly. Don't use a monotonous pitch when talking. Raise or lower the pitch to make certain points in your testimony. Control the rate of speech; be deliberate, but not tiresome. Try to balance volume, pitch, and rate. Listen to yourself speaking and practice when alone—you will only help yourself when it's your time to testify.

Eye contact is very important. Make the jury, prosecutor, or defense counsel feel that you are talking directly to them and not into thin air. Don't start, just find a comfortable place on their face (or above their heads) and keep your eyes there. Don't let your eyes wander as this can make you look dishonest or untrustworthy.

The most important element of speaking is your face. How many times have you thought to yourself, "I don't like his looks" or "He looks sneaky to me"? A jury also forms similar opinions when seeing a witness for the first time. Frowning indicates you are either unsure of yourself (no self-confidence) or unfamiliar with what is going on (loss of control). A "blank" face is one on which nothing but the mouth moves. Wear the same face you use

everyday—be natural. By elevating your eyebrows and letting horizontal lines appear in your brow, you are indicating an interest in what is going on. It also shows self-confidence on your part. When you feel comfortable and wear a natural expression in front of a jury, you'll be trusted, more convincing, and more likely to be believed. You'll appear to be self-confident and in control of yourself and the situation.

Giving your Testimony

Hopefully, you have prepared yourself mentally, emotionally, and physically for testifying by now. You've got the butterflies under control, you know your case (without memorizing it) and you feel confident. So let's go to court and see how to give your testimony in a winning way.

1. First, in your mind, review and practice everything we've discussed so far.
2. Avoid undignified behavior, such as loud laughter, telling jokes, from the moment you enter the courthouse or courtroom. Normally, smoking and chewing gum are permitted in the hallways of courthouses, but not in courtrooms.
3. Stand upright and erect when taking the oath—it shows confidence in yourself and in your knowledge of the case in which you'll be testifying.
4. Control signs of nervousness. There is no reason to be scared or nervous if you've done your homework by reviewing the case carefully and preparing yourself.
5. When you take the oath, you swear that you will tell the truth. DO IT!
6. Speak directly to the members of the jury if it is a jury trial, otherwise, speak directly to the judge. Speak loudly enough so the juror furthest from you can hear you without difficulty.
7. Speak in your own words and do not use slang or police type jargon.
8. Listen carefully to each question and make sure you understand it before you start to answer. Have the question repeated if necessary.
9. Be alert for any question that will lead you to make conclusions (remember, only expert witnesses can give opinions and draw conclusions).
10. Try to answer with a simple "yes" or "no" if possible. Avoid saying "I think," "I believe," "to the best of my recollection" types of answers. You should be testifying only to the facts as you know them.
11. Answer only the question asked, then stop. Do not volunteer any information as your answer may become legally objectionable under the technical rules of evidence. Do not exaggerate anything.
12. Sometimes, you just have to answer "I don't know." There's nothing wrong with this; just minimize doing it.
13. If you find that you gave a wrong or unclear answer to a question, correct it immediately yourself by asking the judge if you can do so.
14. Refrain from showing or indicating emotions such as happiness, joy, disgust, or disappointment about anything that occurs in the courtroom or during the trial.
15. Always be polite and maintain your composure. Do not be argumentative or sarcastic or get involved in verbal fisticuffs with counsel.
16. Finally, the officer who presents honest testimony and maintains a professional bearing during testimony has nothing to fear during cross-examination.

Conclusion

While testifying in court may be intimidating and cause swarms of butterflies to appear in the stomach, learning and practicing a few things will help officers gain self-confidence and present winning testimony in court. Preparation is the key to successful testifying; prepare your case and prepare yourself.

Always review your case before going to court. Know where the courthouse and courtroom where you'll be testifying are located. Go over the facts in your case but don't memorize the case. You will be testifying to facts, no opinions or beliefs. Know the facts as they happened by reviewing your field notes, notebooks, and relevant reports.

Prepare yourself by practicing the proven Dale Carnegie principles of self-development. Practice techniques of public speaking so you'll be comfortable and confident when testifying. When in court, carry yourself with an air of authority, confidence, and self-assurance, but do not look cocky or smug. Stand or sit upright, speak clearly, look directly at the jury, judge, or counsel, and by all means, tell nothing but the truth. If you've done your homework and prepared yourself to testify, you will be an outstanding and credible witness.

Testifying in Court

Quiz

1. The _____ jury is the initial step in the trial process.
2. Most security and police officers do not qualify as _____ witnesses.
3. Know who the major players are: the prosecutor, defense counsel, and _____.
4. The famous _____ way of building self-confidence works extremely well.
5. When _____, what the jurors see is sometimes more important than what they hear.
6. An expert witness is allowed to render opinions and draw conclusions in court. ☐ T ☐ F
7. Probably the most important part of being a successful and confident witness in court is the preparation for testifying. ☐ T ☐ F
8. The petit jury is the initial step at which time the decision to prosecute or not is made based on the strength of the evidence offered by the prosecutor. ☐ T ☐ F
9. When in court as a witness, a security officer should always wear his or her uniform or a business suit. ☐ T ☐ F
10. Officers may not refer to their field notes or notebooks when testifying in court. ☐ T ☐ F

UNIT IX

Customer, Client and Community Relations

This page intentionally left blank

1 Customer Service and the Protection Officer: Guidelines to Achieving Excellence

Randy J. Rice

There have been many challenges through the years in the security profession. One of these challenges is customer service and it is this challenge that many companies are starting to look at very closely. Customer servtice and the protection officer work hand in hand with each other. Most protection officers have a very difficult time with customer service due to the notion "How can the protection officer provide customer service when they are dealing with a large portion of incidents where customers are doing something wrong?" Protection officers can use customer service techniques in everything they do and still have poor customer relations. This chapter will discuss customer service ideas from the beginning and throughout the protection officers' career.

Selection

We must begin with the hiring procedures of the protection officer. When an applicant is being interviewed for a position as a protection officer, the employer should prepare a series of questions to ask the applicant during the oral interview. When addressing this segment of your interview, the first question that should be asked is, "What is your definition of Customer Service?" This will allow you to discern whether you should proceed with the next set of questions. In this profession you will encounter individuals who have never had to practice "Customer Service," and at this point to continue with the subject might be a complete waste of time. However, this would be completely up to the interviewer. At times we see potential in others who can be trained and may turn out to be one of your greatest assets. Also individuals who have not been exposed to this environment do not have bad habits. With proper socialization they may become your greatest Ambassador of Customer Service. Some of the questions that should be asked are scenarios concerning different types of incidents with people that are most common to the place of business. An example of this would be, "How would a protection officer handle a patron of a mall that was smoking in a nonsmoking mall?" Have the applicants explain in their words how they would resolve the problem using customer service skills. Another example would be, "How would you as a protection officer inform the driver of an illegally parked vehicle to move his or her car?" These are just two examples of questions, and questions asked should reflect scenarios related to your specific industry. Once the oral interview is conducted, proceed with a detailed background check. Check the employment history and find out how they have dealt with others they have worked with in the past. Did they have any type of behavior problems while employed with that company? However, in today's employment background checks you will probably find that this information will be limited.

Prior employers may not have or wish to divulge much detail on job performance. This will require the interviewer to study the application prior to the interview. Once a complete and detailed background has been performed and you decide to hire the applicant, customer service training has begun.

Image Enhancement

The next step begins with the image of the company and the protection officer. The new protection officer should be provided with basic information on the job and what is expected. During this stage protection officers should be informed what their role is and how they are involved in the customer service aspect of the company. After providing a detailed explanation of customer service do's and don'ts, the protection officer is ready to move to the next step: the appearance of the protection officer. Appearance is approximately 55% of the message the protection officer sends out to the customer. A protection officer should never underestimate the powers of his or her appearance. As the saying goes "*you never get a second chance to make a first impression*." A professional image speaks well of the employer and the protection officer. Following a few simple guidelines can assist the protection officer in getting it right the first time. These simple guidelines are as follows:

Neat: Shirt tucked in, shirt is neat and pressed, gig line straight, shoes tied and polished, hair well kept and groomed, clean shaven, duty belt kept in order, all insignias shined and clean, equipment working, and worn uniformly.
Clean: Clothing is cleaned and pressed, hands washed, fingernails cleaned.
Jewelry: Simple and not excessive, makeup is light, not too much cologne or perfume.

A person will always respond more positively to someone who appears neat and has a professional manner.

Training and Behavior

The next step is training and training is what "makes or breaks" protection officers and their employer in the area of customer service. Let's start off with some basic examples of how a protection officer can have poor customer service techniques.

- Bad attitude
- Incompetence
- Rumor spreading
- Irresponsibility
- Exploiting people
- Failure to communicate
- Crude speech
- Griping
- Disinterest
- Impoliteness
- Abusive authority

Protection officers want to avoid these at any cost. It is the role of the supervisor and training officers to instruct protection officers on the proper personality traits so they understand how their personality traits and working relations affect themselves and others around them.

Following these seven basic steps will assist the protection officer in maintaining a high regard for customer service:

1. *Taking the Initiative*—Exceptional customer service begins simply by getting involved with something. Make an opening move to show the person care and concern. Keep this in mind whenever dealing with a person; you decide whether you want to act or react. It is your choice and you have to determine which one will best promote customer service. Most places with poor customer service are just *reacting* to a customer, always reacting.

   The protection officer must keep in mind that reacting is tiring, self-defeating, and is usually too late. By acting and taking the initiative, protection officers are able to gain the proverbial upper hand and take the early advantage. People expect others to

react and when the protection officer acts first they are surprised and impressed. An example of taking the initiative would be, you are a protection officer at a mall and observe a young mother attempting to exit the mall and having a hard time opening the doors. Taking the initiative and opening the door before being asked provides a high level of customer service. In this simple act the protection officer has influenced the person's behavior.

2. *Be Positive*—Another choice, once the protection officer has decided to act, is one of these three:
   - Be positive—upbeat, affirming, personable, interested, respectful, and considerate.
   - Be neutral—indifferent, bland, flat, matter of fact, or distant.
   - Be negative—unpleasant, mean, angry, rude, defensive, or uncooperative.

   Being *positive* is where customer service begins to pay off. This gets the relationship started in the right direction. When the protection officer acts, they challenge the customer to react in a positive way. The protection officer must keep in mind that under normal situations the person will respond in a similar behavior. Keep in mind that this may not always be true. The protection officer must remember that when a customer is rude, negative, and generally difficult, the odds are that the protection officer is not the target, just in *range*. If the protection officer comes under attack, do not take it personally. No matter how unpleasant a customer can be, remain positive. Here are some tips to stay positive:
   - Body Language
     a) Keep direct eye contact
     b) Use open body language (no folded arms, hands, legs crossed, hands in pockets)
     c) Smile, Smile, and Smile
   - Voice
     a) Calm
     b) Even tones (not shaky, crackly, or tentative)
     c) Even volume (not too hard, not too soft, just right)
   - Wording
     a) Do not use negative words like "no," "I cannot," or "but"
   - Self-confidence—Most Important
     a) Positive attitude

   If the customer is in a violation of property policy while you have used all of the previous steps, explain why policies have been put into place either for their safety or others. At times the customer's response will explain the reasoning for his or her actions. Try this simple phrase to start the protection officer's explanation to the customer:

   "I understand, however……."

   This scripted response, if practiced, sounds professional. It also informs customers that you are empathetic to their plea. This alleviates the "yeah but……" responses that are so commonly expected from the so-called "security guard," rather than the "Security Professional."

   Postencounter Critique*: After dealing with a customer think of ten things that were done well and write them down.*

3. *Make the Customer Feel Special*—Just keep this in mind: "The customer you make feel special will become a special customer." *There was never a customer who liked being treated like a number*. The protection officer might deal with the same or similar situations ten times a day, but each encounter remains a special and personal matter to each new customer the protection officer deals with. The idea is simple. Just provide such remarkable service that you surprise the customer and people around them. Make the customer feel honored by going above and beyond the call of duty. If the officer approaches each and every customer *like they are your only customer*, they will stay satisfied and happy. Make the customer feel important and do not overdeliver in the way or manner you help them. The protection officer must

remember that they may not be able to fully help the customer or give the customer what they ask for, but you can make them feel special. When the protection officer does this, it makes the customer more tolerant and they become more open minded, forgiving, and kinder toward you. *The protection officer must remember, the easier the customer is to work with, the easier the job will be for them.*

4. *Listen and Understand*—The first thing the protection officer must do is to identify the problem and focus on the customer. Give the customer 100% attention. The protection officer must concentrate on getting "in tune" with the customer, finding that same wavelength. Make that person's point of view your own at that point. The protection officer must demonstrate interest in understanding the situation. They must also establish a common ground by looking at things from the customer's perspective.

   If you were that person what would you want?
   Think Like a Customer!

   The protection officer should sniff out the other person's concerns, wants, and needs. Ask questions in order to obtain facts and listen carefully. Try to read between the lines, because the customer may be confused or lack necessary facts or simply cannot explain things well. Pitfalls the protection officer needs to avoid are as follows:
   - jumping to conclusions
   - prejudging
   - placing blame
   - arguing
   - becoming defensive
   - starting to solve the problem before analyzing it

   The protection officer should welcome bad news with open arms. Problems give the protection officer a chance to leave a mark on the mind of a customer. They can turn them into real opportunities. It is an opening for the protection officer to do something special.

   Listening, however, is always the hardest and most important part of this step. Here are a few tips to assist the protection officer with developing good effective listening skills:

   ### *Don'ts*

   - Interrupt the customer.
   - Look away from customer.
   - Doodle, pace, frown, or make strange facial expressions.
   - Put words in the customers' mouth or attempt to finish their statement.
   - Answer questions with a question.

   ### *Do's*

   - Hear the customer out, concentrate on what is being said.
   - Maintain direct eye contact.
   - Let the customer know you are paying attention.
   - Paraphrase to clarify.

   Of all the don'ts and do's listed above, the most important "do" is paraphrasing what the customer has informed the officer on. Simply restate what the customer has said in your own words. Paraphrasing is important as it demonstrates to the customer that the protection officer was paying attention and understands what they have told the officer. It provides the customer and the officer with the opportunity to clear up any misunderstandings or gaps in the communications process.

   Please note that paraphrasing is only to ensure and demonstrate understanding, not to state a position or try to solve the problem.

5. *Be Helpful*—Once the protection officer has truly listened and through paraphrasing has a good handle on the situation, the protection officer now knows what the customer's

expectations, wants, needs, or concerns are. Now the officer can address the top priorities. The protection officer should take personal responsibility for satisfying the customer. Protection officers should consider themselves an agent of the customer. For a brief moment, be on the customer's side and put both heads together and create options. Search for alternatives to the customer's problems. Do some joint problem solving, keeping in mind the resources that can be brought to bear on the situation, because the officer has a better idea of what is available to work with than the customer does.

The idea of this step is simply to help, or, in the case of a problem or complaint, to fix things. Whatever the need, take care of it following the company's policy and procedures. Provide help even if it is the customer's fault and avoid pointing the finger and run-arounds. Just put forth the effort that clearly says, "The buck stops here." *The protection officer will always be able to help the customer in some way.* Sometimes the protection officer cannot give the customer everything they want, but every time the officer can give something the customer wants, they walk away pleased and feeling good. Never dodge problems. Do not think of them as an aggravation, but as a valuable opportunity. This is one of the important "moments of truth" in customer service. Customers who have had their problems and complaints handled effectively will become the company's most loyal customer and probably the most pleasant ones. They will trust and believe in the officer as well as his or her employer.

6. *Follow-up*—This is the part where the officer takes the personal responsibility for the customer and makes sure that the plans the officer has made and the actions that the officer took made a difference. If the protection officer is simply answering questions, it can be made simple by asking if there was anything else you could do for them? Provide the officer's name and tell the customer that if he or she needs anything in the future to please contact him or her. If the customer has a problem or a more complicated request, it could involve offering to follow-up with a phone call or asking a supervisor if he or she remembered to take care of the things on his or her end.

   There are many different approaches that the protection officer can use to seize the initiative, be positive, and make the customer feel special. Likewise, various alternatives can work as the officer tries to understand, offer help, and follow-up. Think about what works for the officer, what more or less comes naturally, what the officer can do well. Do not try to be someone else. Customer service, as the protection officer provides it, will reflect on the officer's individual style—one's very own magic touch.

   Finally, when dealing with angry customers remember the following tips:

   - Let them vent.
   - Do not get emotionally involved.
   - Do not rationalize or justify.
   - Be empathetic.
   - When all else fails:
     a) Make them aware of their behavior.
     b) Say, "I would like to help and I will when you can calm down."
   - When the officer has stuck to the basics, draw that line and call the supervisor.

7. *Become approachable:* Remember you are a figure of authority. No one at any given moment thinks of you as just an employee. Customers, guests, and patrons know that your job is to enforce both policies set forth by your company and laws that your state has passed. However, if the protection officer is approachable utilizing all of the tools set in place in the previous steps, guests will consider you an ally, one that they can go to with any situation, giving the guest a feeling of safety, security, and peace of mind. The guest will know that you are there not only to protect them but to serve them as well.

   Remember when dealing with negative guests there are always others watching to see how you are handling the situation. The question in your mind is:

   Am I going to remain professional or will I get pulled into a battle of wits?

   Remaining professional is what you get paid for, and will impress valued guests. Remember the adage:

   "Calmness is contagious."

Telephone Personality

No matter what position a person holds in a company, they have to spend time on the phone. This is one of the most powerful tools at one's disposal. When making or receiving phone calls, the officer is representing the entire organization. To a caller, the officer is representing the whole company. When a caller finds a competent, courteous, and efficient person on the other line, they are likely to form a positive and lasting impression of the organization. When people cannot see the officer, as one on the telephone, the customer only has a voice to deal with and make them feel comfortable. Tips to improve the officer's phone personality include the following:

- Provide full attention to the caller.
- Use enthusiasm as a tactical advantage.
- Deal with the customer like they are right in front of the officer.
- Use simple straightforward language—no slang or technical terms.
- Talk directly into the mouth piece.
- Use the caller's name; if unsure ask for it.
- Always thank the caller at the end of the conversation.

When using the phone sit up straight, keep the head held high, and smile while speaking.

Using the few tips above will provide the officer with confidence and heighten the customer's confidence in the officer.

Telephone Standards

It is essential that the protective service organization establishes a set of telephone standards the officer can use:

Answering the Phone

- Answer the phone by the third ring—be timely and alert.
- Use a friendly greeting:

  "Thank you for calling _____. This is Officer _____ speaking. How may I assist you?"

- Always get the customer's name.
- Talk slowly and distinctly.
- *Be helpful.*

Putting a Caller on Hold

- Usually there are three reasons to put a caller on hold:
  a) Already on the phone with another person.
  b) If the caller would like to speak with someone else.
  c) Obtaining information for the caller that is not readily available.
- In any case the officer must always ask the caller if they would mind being put on hold.
- If the caller elects to be placed on hold, thank them.
- If they are going to be on hold for a long period, pick up and let them know they have not been forgotten.

Ending a Call

- Always end the call with a positive statement:

  "Thank you for calling. If I may be of further assistance please let me know."

Summary

In conclusion, this chapter has touched the surface of customer service and the protection officer. It discussed the beginning stage of customer service from the hiring process to training of the protection officer. There are various types of training classes a protection officer should go through, and that are available; however, following the guidelines set forth in this chapter will greatly assist the protection officer in achieving the goal of excellent customer service. Customer service will always continue to be a challenge for the protection officer, now and in the future.

Customer Service Checklist for Protection Officers

Yes No

- Did I have a professional image?
- Did I avoid poor communications traits?
- Did I listen clearly?
- Did I paraphrase properly?
- Did I take initiative?
- Was I positive?
- Did I use correct body language?
- Did I keep good eye contact?
- Did I make the customer feel special?
- Did I understand the message?
- Was I helpful?
- Did I follow-up after the situation?
- Did I use good telephone techniques?

Bibliography

Crown America Corp. (1997). *Customer Service Excellence Training Material*.
P. Satterfield (1989). *The Security Officer's Performance Manual*, Cypress, CA.
D. Salter (1998). Interview—*Public Relations and Security*.
C. Thibodeau, C. Hertig, and G. Barnett (1998). Public relations. In *Protection Officer Training Manual* (International Foundation for Protection Officers), Woburn, MA: Butterworth-Heinemann.
J. Wanat (1981). *Supervisory Techniques For The Security Professional*. Boston, MA: Butterworth-Heinemann.
J. Wilson (2007). Personal Communication.

Customer Service

Quiz

1. The protection officer can use customer service techniques in everything they do and still have poor customer relations. ☐ T ☐ F
2. It is a good idea during the hiring/interview process to prepare a series of scenarios in which customer service skills must be applied and addressed to determine the level of ability of the potential employee. ☐ T ☐ F
3. Appearance represents what percentage of the message the protection officer sends out to a person?
   a) 5%
   b) 75%
   c) 55%
   d) 90%

4. You never get a second chance to make a first _____.
5. Poor customer service techniques might include the following. (Select the best answer)
   a) Impoliteness
   b) Irresponsibility
   c) Bad attitude
   d) All of the above
6. Paraphrasing is important as it demonstrates to the customer that the protection officer was paying attention and understanding what they have told the officer and it provides the customer and the officer with the opportunity to clear up any misunderstanding or gaps in the communication process. ☐ T ☐ F
7. It is not essential that the protective service organization establish a set of telephone standards that the officers use. ☐ T ☐ F
8. Taking the _____ and opening the door before being asked provides a high level of customer service.
9. Give the customer what percentage of attention?
   a) 25%
   b) 50%
   c) 100%
   d) 95%
10. It is the role of the _____ and _____ to instruct protection officers on the proper personality traits so they understand how their personality traits and working relations affect themselves and others around them.

2 The Supervisor's Role in Improving Customer Service

Christopher A. Hertig

The asset protection/security supervisor is a key player in both establishing and maintaining an appropriate customer service orientation within the protection force. To better understand how the supervisor functions, we must first examine the role of the supervisor and then assess the development of an organizational philosophy.

Role of Supervisors

- The person who represents higher authority—the *core philosophy* of the organization—to subordinates. Supervisors are the links between management and line officers or loss prevention agents.
- The person who must ensure compliance with policies and procedures and quality performance in the customer service area.
- The individual who is the first responder to any and all situations—as such a supervisor must be a model diplomat. He or she must demonstrate diplomacy in trying circumstances, such as accidents, investigations, personnel issues. He or she must work when there are competing interests involved. These can be subordinates, other departmental supervisors, higher management, customers, law enforcement agencies, etc.
- A master of communications, especially interdepartmental and interagency communications. Again, other departments (human resources, physical plant, etc.) and external organizations, such as local police, vendors, clients, and regulatory agencies, must be dealt with.

Core Philosophy of Parent or Client Organization

In order to gain a firm foothold in public or customer relations, one must first understand what the philosophical foundations are within the parent or client organization. Each organization is different; they do not simply all want "to make money" as the uninformed may believe. Each organization may indeed want to make money but in its own manner. Each takes a different path. Some rely on innovations in technology. Some work on customer loyalty. Others focus on cost containment. Still others place great emphasis on close ties to the community.

Whichever guiding beliefs lie at the center of the organization, these must be firmly understood by those who wish to effectively represent that organization to customers. A key question to be addressed is:

What makes my employer and/or client unique from other organizations in the same field of endeavor?

Organizational philosophy is founded in the history of the concern. Each organization is established at some point and evolves over time. The original beliefs may be modified

somewhat, or they may remain unchanged and be further cemented into the organizational culture. Whatever the case may be, an important question to be asked when studying an organization's culture is:

What is the history of my employer?

This is especially important for security service firms. Some of them such as Securitas (which acquired Pinkertons) have an illustrious history. One could probably develop a three credit college course on the contributions of Alan Pinkerton. He was a prominent citizen who played a key role in the history of the United States and the development of investigative practice. Smaller newer firms may also have founders and principals who were industry pioneers. Each organization has a unique history that can illustrate important lessons. *Knowing this history helps to make each officer a more effective company representative*. Unfortunately, this may not be capitalized upon as effectively as it should be.

Organizational philosophy is framed in the policies of the organization. Reading and understanding these policies is essential to comprehending the philosophy of the organization—as well as knowing what the rules are to be enforced. A question to be mulled over is:

What do the policies of my employer state?

Organizational philosophy is more precisely articulated in the procedures of the concern. These specify the "what" and "how" of the policies. They state how the policy, the philosophy, is executed. When reading procedures, some introspection can be given to the following inquiry:

What do the procedures explain?

Once policies and procedures are fully comprehended, it becomes necessary to examine the role of the security department in advancing the organizational philosophy. Upper management has delegated certain functions to the security department. Efficient use of resources and organizational survival mandate that the following question be addressed:

What is the role of the asset protection/security department in advancing that philosophy?

Ensuring Optimal Performance and Adherence to "Best Practices"

Supervisors must ensure that their charges perform to the best of their ability. They must also work to achieve quality through adherence to recognized standards of performance or "best practices." There are several steps to take toward this end. The first step is to conduct a job task analysis to determine roles and functions of officers. Once this is done, a clear picture emerges as to what officers do, what their key competencies are. From there, recruitment, selection, training, and the remainder of the human resource management process can occur.

The Customer Service Role of Protection Officers

Protection officers are often highly involved in public relations/customer service. At a seminar given some years ago by this writer, an officer stated that "public relations is 90% of this job." It was interesting to note, as the class was at a manufacturing facility where public/customer contact is not as great as it would be in a shopping center, college campus, park, or office building.

Another interesting anecdote occurred while reviewing the responses to a curriculum study done in 1985. The study was an attempt to identify a generic security officer training curriculum. It consisted of a literature review followed by a questionnaire sent to randomly selected security managers from the ASIS membership directory. The questionnaire asked the respondents to rank which topics they felt were most important. There was also room for additional comments. One respondent felt that public relations was the most critical area for a security officer to be proficient in as that officer's interaction with others determined how a negative event was perceived; that no matter how bad a situation was, the officer's public relations skills was the critical factor in how bad it was felt to be. Such an observation is certainly relevant to emergency management!

Some organizations such as shopping centers, hotels, and amusement parks utilize security personnel as customer service agents to a large extent. Sam's Clubs "greeters" serve to welcome a customer into the store while at the same time ensuring that they are members. In many hotels a similar function is performed by protection officers in the hotel lobby. Lounges employ "Lounge Hosts" to welcome customers and keep out troublemakers. The sample job description given below for "HAPPY TIME RESORTS" provides ample evidence of the customer service role for security personnel:

Job Title: Lounge Host
Organizational Unit: Asset Protection
Accountability: Security Shift Supervisor
Job Summary: To provide for a safe, enjoyable atmosphere for our guests.
Duties and Responsibilities:

1. Greeting customers in the Lounge.
2. Controlling access to Lounge.
3. Maintaining an accurate customer count.
4. Ensure the safety of the Lounge and the surrounding area.
5. Maintain order in the Lounge.
6. Ensure compliance with Alcoholic Beverage Commission regulations.
7. Customer assistance as appropriate.

Interaction: Lounge manager, Bartender
Prepared By: Director of Asset Protection
Approved By: Vice-President, Human Relations

Required Licensing, Certifications, Training

Training and certification of protection officers. Specific, *recognized* and *documented* training of protection staff is essential to projecting a positive image. It is also integral to making officers competent to provide a meaningful level of service.

State and provincial licensing or certification. This is essential where required by law. It also helps to give the protection force recognition. While there are serious deficiencies in state training and licensing requirements (the failure of most governmental entities to regulate proprietary forces, as an example), there is likely to be more regulation in the future: licensing may be attractive as it provides a revenue stream to the state, county, or city. Astute managers should see the direction that legislation is taking and be both proactive and supportive. State-mandated standards are generally minimal in regards to training and screening. Professional managers ensure that their organizations go beyond the minimal and embrace "best practices."

Company certification. These credentials are given by private companies, generally in the use of equipment or techniques. Some examples of company certification programs common within the protective services arena are the Crisis Prevention Institute, PPCI Training, Inc. Each company establishes its own criteria for certification and sells its services to customers. These certifications may be important as they are "best practices"; only those organizations interested in being on the leading edge of professionalism embrace these programs.

Of note is the use of instructor certification programs. PPCI Training, Inc. and CPI have instructor certification processes where an individual becomes certified to teach. Having one or more individuals certified as instructors who teach nonsecurity staff is a valuable customer service within an organization. Having Certified Protection Officer Instructors on staff can be a valuable customer asset for security service firms who may wish to offer training to clients.

Professional certification programs such as the Certified Protection Officer (CPO) and Certified Fraud Examiner (CFE). Similar to company certifications, attaining these credentials affords one industry recognition. Security staffs that are professionally certified are at a higher level of professional development. As such, they are providing more service to their customers. Professional certifications make one stand out; they enable the organization that has certified employees to demonstrate a superior level of professional development. This is markedly different than simply claiming professional status without proffering any evidence. Having

professionally certified staff members is a very powerful marketing tool as G4, Securitas as well as some smaller firms have discovered.

Industry certification. This includes such things as the International Association of Health Care Security and Safety's Basic Standard. This is a definite standard within healthcare protection that should be obtained by security forces. As specialized, vertical market sectors of security grow and develop, more of these types of programs may appear. The International Association of Campus Law Enforcement Administrators has established a Campus Protection Officer program. As the needs of campus asset protection are unique and relatively few schools have police academy trained staffs, this program will probably become heavily utilized.

Systematic, automatic professional development is necessary! For employees to function at optimal levels, they must be constantly learning. There are several programs that aid protection supervisors and managers in this regard:

- The *Safety Standard of the IAHSS* is a logical means of organizational development for healthcare protection organizations. The Safety Standard helps to enhance the safety orientation of protection officers so that they can provide additional services. This not only expands the services of the protection organization but also presents them in a more positive manner. No longer is security seen as a paramilitary, law enforcement type organization. Instead they are viewed more as helpers. And "helpers" who assist the parent/client firms in complying with OSHA regulations are a valuable asset.
- The *Professional Security Training Network (PSTN)* offers subscribers monthly training tapes. Each month a different topic is covered so that a subscriber firm can enjoy continuous professional development for its staff. Tests are also included with each month's tapes so that learning is measured and employees are not simply "watching tapes."
- AST Corporation has a series of program available online and on CD-ROM. Courses on retail, homeland, physical, and special events security can aid in staff development. These programs can help to develop specialties within a security organization as well as new career paths for the officers and agents.
- Periodic guest speakers from police departments, local colleges, and civic organizations (Red Cross, Chamber of Commerce, Volunteer Fire Department, etc.) can also aid in continuous professional development. Much of this is essentially free training. Having representatives of these organizations speak to protection forces also raises the level of visibility of the security department.

Feedback Loop: Audits, Customer Complaints

The quality assurance aspect of the supervisory process can be accomplished via two different evaluative techniques: audits of individual officers and an analysis of customer complaints. Audits can take the form of "shopping" an organization by having someone unknown to the protection officer ask for directions or assistance. Phone inquiries can also be made and the results of each contact documented. Investigators can use predesigned forms to rate pleasantness, appearance, knowledge, responsiveness, or any other criteria deemed to be important.

While a formal assessment performed by an independent entity may be preferable, and indeed quite appropriate, to large protection force operations, informal audits can also be used. The latter are much more common and easy to implement. Care must be taken, however, not to use slipshod methods when evaluating or disciplining an officer.

Customer complaints are another source of valuable intelligence. Inappropriate customer service practices, such as surly officers, can be detected through customer complaints. More importantly, systemic deficiencies such as inadequate staffing levels, substandard procedures, shoddy maintenance, or poor personnel traffic flow patterns can be spotlighted. A series of complaints focused on a particular area gives managers a clear signal that something is amiss. The challenge is to design a system where the information (complaints) can be easily retrieved, analyzed, and acted upon. Interdepartmental relations may be key here as personnel

in other aspects of the organization may be aware of the problem areas. Meeting with them and having open lines of communication can keep the security department apprised.

For More Information

Layne Consultants International (Layneconsultants.com or 303/377-2176) offers a seminar on customer service.

The Professional Security Training Network (www.twlk.com/security/ or 800/942-7786 has numerous video programs on public relations, customer complaints, etc.

The Office of Community and Professional Development at York College of Pennsylvania (www.ycp.edu or 717/815-1451) offers a seminar on customer relations as well as one on crowd management.

The Supervisor's Role in Improving Customer Service

Quiz

1. The asset protection/security supervisor is a key player in both establishing and maintaining an appropriate customer service orientation within the protection force.
   ☐ T ☐ F
2. Knowing the organization's _____ helps to make each officer a more effective company representative.
3. Supervisors must ensure that their charges perform to the best of their ability. They must also work to achieve quality through adherence to recognized standards of performance or "_____."
4. What percentage of an officer's job is related to public relations?
   a) 10%
   b) 50%
   c) 30%
   d) 90%
5. Specific, recognized, and documented training of the security department personnel is essential to projecting a positive image. ☐ T ☐ F
6. For employees to function at optimal levels, they must be constantly _____.
7. Having guest speakers from police departments, representative from local colleges, and civic organizations (Red Cross, Chamber of Commerce, Volunteer Fire Department, etc.) can aid in continuous professional development.
   ☐ T ☐ F
8. Astute managers should see the direction that legislation is taking and be both _____ and _____.
9. Understanding the organizational philosophy is important only to the management team. ☐ T ☐ F
10. Some examples of organizations that may utilize security personnel as customer service agents to a large extend may include: (Select best answer)
    a) Shopping centers
    b) Hotels
    c) Amusement parks
    d) All of the above

This page intentionally left blank

3 Tenant Relations

Glen Kitteringham

This chapter will introduce the reader to tenant relations and how it has a strong supporting role to play in the successful implementation of a site security program. Furthermore, several concepts including discrete sites, environmental and social crime prevention theory, and community policing as they relate to security will be discussed. The reader will learn how tenant relations, good and bad, affect the security program. Finally, an overview of terrorist threat and criminal activity indicators will be presented to help security professionals look for such activity at their site.

There are at least six reasons why the Security Manager/Supervisor should consider good tenant relations as a cornerstone of the site security program:

1. There will never be enough security staff available to help protect a site.
2. Tenants, in a passive role, can be the eyes and ears of the security department and as there are many more of them than security staff, can provide considerably more information.
3. Tenants can play an active role by keeping doors locked, challenging strangers, educating visitors of security rules and regulations, and helping out in extreme situations such as emergencies.
4. Their presence alone is often enough to deter undesirable or criminal activity.
5. Tenants often provide solutions to security and life safety issues that security personnel may not have thought of.
6. Finally, tenants may own a considerable amount of property on site; therefore, they also have a personal responsibility to help protect it.

With the growth of large single-use sites, or as they will henceforth be referred to as "discrete sites," and both the increase in private security due to "the growth of mass private property" (George and Button, 2000, p. 34) put in place to protect these sites and the inability of public policing services to provide services at the same level as previously (Marquis, 2000, p. 28; Christie, 1994, p. 108), the need for a comprehensive asset protection plan provided by private security is vital. Furthermore, proactive security managers/supervisors must use every source at their disposal to enhance the asset protection plan and, as identified in the opening paragraph, tenants can be of great benefit in the overall plan.

Consider the following scenarios in determining whether tenant relations had a role to play in making the security professionals' job easier or harder.

> In a retail mall environment, employees and customers in a nightclub would consume alcohol until earlier in the morning on a daily basis. Many of them, inebriated, would access the mall via the entrance where they would create disturbances, open exterior doors to street people, not to mention the potential for slip and falls where people could easily get hurt. Despite repeated requests from security staff and building management for the nightclub management to contain the activity, the staff and customers continued this activity for many months.

In a large commercial high-rise, a restaurant was open past midnight daily. The restaurant became a hangout for a gang who was responsible in the neighborhood for several brawls that spilled out into the street on a regular basis. In addition, illegal drugs were reputed to be sold from the location. Repeated requests to restaurant management to control the activity went unanswered. It was not until the restaurant went bankrupt and closed its doors did this activity stop.

A tenant in an office complex was repeatedly victimized by laptop thieves despite security requesting the tenant to increase physical security in the area. Finally, the tenant was convinced after several break-ins. Not only was the tenant's initial nonchalance inviting the thieves back time and time again, they were creating the situation where other tenants were in danger of being victimized.

At an office structure, the company was victimized but after the first break-in, a joint security audit between the tenant security representative and building security identified several areas requiring repair or enhancements. The tenant increased physical security levels to the point where thieves were unsuccessful in any more theft attempts.

At a site, where an impending major political event was set to transpire, joint tenant and facility security were able to effectively work together from the outset, allowing the entire facility to act as one in their responses by developing Standard Operating Procedures for both parties. As a result the facility was well prepared to respond to any protest-related security issues.

In a facility, tenants refused to support building security who wished to provide life safety, fire warden, and building evacuation training. As a result, tenant employees are ill prepared to respond to legitimate emergencies in the building. Evacuation times are poor, complaints from building residents are constant, and security personnel are frustrated and constantly unfairly criticized.

A shopping mall had a tenant who provided social assistance to locals. They happened to be located immediately adjacent to a liquor store. When money was provided to those in need, some of them would go next door and spend the money they received on alcohol. These locals would often wander about the mall into restricted areas including back corridors and stairwells to consume their purchases. In many cases they would cause disturbances throughout the entire site.

A shopping mall tenant had such a poor relationship with the security department, each time the bike patrol would ride by his storefront, he would complain to the building management that security was in danger of running his tenants over with their bikes. This poor tenant relationship wasted everyone's time, and reduced the effectiveness of the security department personnel as they were forever defending themselves from the tenant's accusations. The property managers spent valuable time refereeing the situation and the tenant, instead of providing services to mall customers, spent his valuable time accusing the security department of incompetence.

Good tenant relations with several tenants allowed the department to defend itself against accusations of poor performance during building evacuations. In a room full of fire wardens after a building evacuation, several tenants defended security personnel from other fire wardens after they complained security were not taking everyone's concerns seriously. The difficult situation was diffused and people were able to discuss the evacuation without emotion and resolved it to everyone's satisfaction.

An argument between a retailer and site security led to several years strained relations over the legal liability of security personnel arresting shoplifters. The security manager could never convince the retailer that security staff could not arrest shoplifters based on the retailer's parameters but had to be based on criminal code requirements. The retailer insisted that the security manager not allow his or her staff to arrest. This decision was based on poor personal relations, not legal restraints. This led to the retailer constantly complaining for several years to the property management that he was not getting value for the rent he was paying. The situation resolved itself when the retailer moved from the site.

The security program a protection professional creates is only as effective as the people assigned to implement it. In many cases, particularly in facilities where there are large numbers

of individuals, security and safety is everyone's responsibility. This chapter will focus on those large properties where there is a tenant base as part of the make up of the site. As a result, several concepts will be introduced to readers to familiarize them with the overall direction that the chapter moves in. Environmental crime prevention, social crime prevention, discrete sites, and community policing will be discussed in some detail in the following sections.

"Environmental crime prevention" focuses on the specifics of the crime, whereas "social crime prevention" focuses on the root causes of crime. Both social and environmental crime prevention impacts and, in turn, are impacted by security professionals. Furthermore, tenant relations (interactions between the property manager and tenants, regardless of whether these relations are positive or negative) are also about "micro-community relations" and community policing or, in the case of private security, "community protection."

> "*A short and simple explanation of environmental crime prevention is that crime control practitioners focus their attention and energies upon potential locations of criminal activity.*" (Minion and Davies, 2003, p. 179)
>
> "*Social crime prevention aims to prevent people from drifting into crime by improving social conditions, strengthening community institutions and enhancing recreational, educational and employment opportunities.*" (Introduction to Security and Crime Risk Management, Module 1, University Leicester, England 1999, p. 227)

While this second statement refers to society as a whole, as will be pointed out in the following pages, there is no reason it should not be applied to large private property sites, such as transportation hubs, including seaports, airports, train, bus, and ferry terminals and stations, casinos, hotels, shopping malls, residential and commercial properties, hospitals, universities, housing projects, and other so-called "discrete" sites. One definition of a discrete site is a "predefined area/structure with unique characteristics that differentiate it from surroundings." Another less formal definition is that a discrete site is "a really big place with a single name" (Kitteringham and Dallas, 2001) like the "University of Alberta," the "Calgary International Airport," or the "West Edmonton Mall." There may be a single or dozens of buildings, hundreds of service providers, including retailers, food services, and distinct functions, and thousands of daily users, either one time or repeat users; however, they all come together in a single location for a common related purpose.

An example of a discrete site is the aforementioned "West Edmonton Mall," North America's largest mall. It has two indoor amusement parks and a marine mammal park. The mall has an average population of 60,000 people per day, increasing to 200,000 on Saturday and on any given day there are 10,000 people on site consuming alcohol. The security service receives on average 40,000 calls for service per year. There is a department of 50 security staff including a gang squad intelligence unit (Murphy and Clarke, 2005, p. 243). The mall itself covers an area of 5.4 million square feet with over 600 stores and services with parking for more than 20,000 vehicles, which makes it the largest parking lot in the world. More than 23,000 people work in the mall. It receives 22 million visits a year (http://en.wikipedia.org/wiki/West_Edmonton_Mall). Additionally, it has an 11-story hotel with conference facility and a skating rink where the NHL Edmonton Oilers Hockey Club practices from time to time.

How then does the security manager/supervisor work with all the people working at this "discrete site" to maximize asset protection and minimize service losses? For starters there is no reason why security professionals cannot take a page out of the community policing handbook. According to the Community Orientated Policing Services:

> "*Community policing focuses on crime and social disorder through the delivery of police services that includes aspects of traditional law enforcement, as well as prevention, problem-solving, community engagement, and partnerships. The community policing model balances reactive responses to calls for service with proactive problem-solving centered on the causes of crime and disorder. Community policing requires police and citizens to join together as partners in the course of both identifying and effectively addressing these issues.*" (US Department of Justice, COPS Website)

Just as police recognize the value of engaging the community in crime prevention strategies, so too should security professionals be willing to engage the discrete site community in the same strategies. Discrete sites are no different from the wider community other than the size of the geographic site boundaries or spatial definition of the location.

The security model also calls for proactive problem solving focusing on the local crime and disorder. Protection of assets requires security and tenants to work together as partners in reducing opportunities for crime to occur both from a physical and procedural perspective. Lest one think a security professional's only responsibility is crime and disorder, this is a good place to remind them that there are others issues they must take into account. One such loss prevention model is the WAECUP acronym. It stands for **W**aste, **A**ccidents, **E**rrors, **C**rime and **U**nethical **P**ractices. The security professional at times needs to be reminded that there are issues other than crime and social disorder. The same strategies apply with these other issues. One must give thought to how tenants can be brought into the mix in order to maximize the protection of assets. This must be done to a certain extent discretely as tenants can argue, quite rightly, that their employees are not to do someone else's (security) jobs but their own.

Discrete sites are often cities in their own right with all the services and amenities found in the larger communities. Power generation or at minimum emergency power capability, protective services, janitorial, and food services are just a few of the services found at the discrete site. With this wide variety of services comes a large population. Combining the services with the assets and the people requiring protection gives security personnel a large responsibility. Just as in the wider community, there will often be a communication network in place to reach the discrete site's community. This network may consist of people communicating in the old fashioned way of face-to-face, telephone, e-mail, blackberry, emergency broadcast, or a combination thereof.

So, how does a security manager/supervisor create community and situational crime prevention programs? For starters, a solid understanding of the site, what services it provides, and solid security incident data capture and analysis are vital. Security programs must be based on legitimate, specific, and actual incidents occurring within the site. Security staff must document the various situations, incidents, and calls for service they respond to. While there is the reliable standby of pen and paper, when it comes to reviewing security incident data, it is time-consuming. There are several electronic report writing programs available in the marketplace and it is recommended that if a site is not utilizing such a system, then security professionals should investigate the feasibility of introducing such a program as soon as possible. The collection and review of data is of vital importance as it provides factual evidence of what is transpiring at the site. It provides evidence of what is actually happening as opposed to what people "think" is happening, often two vastly different things. This is where the security manager/supervisor should initially concentrate the resources. The role tenants and good tenant relations play in this is obviously determined by what comes out of the data capture and analysis process. Of course, anecdotal information and good communications between tenants and security can and should be pursued. A proactive security manager/supervisor should not wait for an "official" request for service or until an incident occurs before exploring problem solving within the discrete site community. Many occurrences influence the tenant and will have a huge impact on tenant relations. If security staff are proactive, legitimately concerned about the site, are problem solvers, take tenant security and life safety concerns seriously, and implement practical suggestions to make the site a better place to work then good tenant relations should follow.

Following this, there must be trust between tenants and security. In addition, security staff must see themselves as "enablers of service" on behalf of tenants. Security professionals must understand that they, just like every other service provided by the property manager, are there to enhance the customer experience. Some security professionals may disagree with this analysis but it remains nonetheless one of the principle reasons for their existence at the site. Regardless of the discrete site's service, whether it is an airport, shopping mall, casino, hospital, or commercial high-rise, security is provided to make the site an attractive place to want to do business. Granted, a hospital is hardly the same as a shopping mall. Hospital "customers" are not there by choice (in most cases) but the mandate of security, which is

to provide a safe and secure environment for patients, visitors, employees, contractors, is the same mandate security professionals at shopping malls, commercial high-rise properties, sports arenas, and every other discrete site provide.

Another primary function of the security department is to protect the site as it is an investment of the owners (Johnston, 1992, p. 102). Regardless of whether it is owned by a private or public entity, whether it is a not-for-profit or for-profit organization the asset must be protected. At times it must be protected from tenants, and their actions or lack thereof whether deliberate or accidental. Good tenant relations are critical as there must be a level of trust involved that allows communication between the parties to work through whatever difficulties may occur.

Another primary function of the security group personnel is that they are on site to protect the tenants and their customers. Unfortunately at times building security will be at odds with tenants for several reasons. These reasons include the following: multiple tenants occasionally have differing agendas; some tenant activity may actually generate undesirable activity; tenants may not have the time, inclination, or money to do what is expected of them; or sometimes they simply do not care what building management or security wants or needs.

So, back to the original question: how does a security professional create a crime prevention program for the site that capitalizes on tenant relations? For starters, it is always easier to divide a large, seemingly overwhelming job into a series of smaller, easily manageable jobs. Logically, what follows is to identify your site customers into easily identifiable groups. For example, in a commercial high-rise, there are readily distinguishable groups (with some overlap). There are tenants who work in the building, contractors who provide services to these tenants, and visitors who are conducting business with the tenants. Then the tenants can be subdivided further into retail and tower. Retail tenants are obviously those who provide a variety of services to both building residents and those coming in from off the street. Depending upon the make up of the commercial high-rise, where in the city, province/state, or county it is located, there will be a variety of retail services provided. There may be bars, nightclubs, restaurants, food kiosks, financial institutions, medical services, liquor stores, sporting goods stores, electronics stores, communications stores, and drycleaners, along with a whole host of other services.

For the shopping mall, the wide range of retailers will be dependant on the scope and size, which ranges from small neighborhood malls to West Edmonton Mall or the Mall of America. When it comes to these malls it may be appropriate to divide the security program into retailers who have their own in-house or contract security providers and those who do not. Obviously, if an anchor tenant has his or her own security department it makes sense to coordinate his or her portion of the overall crime prevention program through hi or her. It is doubly important to have positive working relations with the store security department as they can have a huge impact on the effectiveness of the program. For other discrete sites, it is up to the security professional to determine who the clients are and whom they are working with.

The next thing to be determined is the type of medium to be used. Will flyers, e-mail, in-house close circuit television system, face-to-face meetings with tenants in large groups or one-on-one meetings, radio, handouts, "snail mail," Website, posters, etc. or a combination thereof be used? Likely one type of communication medium will not work for all tenants and it will be up to the security professional to determine how to get the best response from each tenant. One example of a much more commonly used communication method is closed circuit television network that the property manager has access to conduct advertisement. Usually tenants will pay for air time to advertise sales, services, or community services. There is no reason that security should not be able to access this service to broadcast messages about locking vehicles, locking offices, reminding tenants that the security department conducts escorts for employees or site users, and a whole host of other messages. As many property managers shy away from broadcasting specific issues such as there have been "X" number of car prowlings in the parkade, the security professional should consider a softer sales approach when warning site users. For example, the message that is broadcast could remind site users to lock all belongings in the trunk of the vehicle to make the vehicles less attractive to theft. The message is similar, it is just the second one is less threatening.

If we take the community policing statement and simply replace the words "community" and "police" with "tenants" and "security," along with a bit of artistic license, then it becomes quite simple in a discrete site where security professionals work with the tenants to create an asset protection program.

> *The tenant security program focuses on crime and environmental & social disorder through the delivery of security services that include aspects of traditional protection strategies, as well as prevention, problem-solving, tenant engagement, and partnerships. The tenant security model balances reactive responses to calls for service with proactive problem-solving centered on the causes of crime and disorder. It requires security professionals and tenants to join together as partners in the course of both identifying and effectively addressing these issues.*

Just as the case were in the larger community, not all concerns the community has are passed directly onto the police; there will also be issues where all tenants are not necessarily going to call security with every issue even when they should. In some cases, security professionals are going to have to work hard to educate tenants as to their responsibilities when it comes to the overall site protection program. Security professionals will have to gain the trust of tenants and respond to their concerns; in some cases, this may take years and, unfortunately, in a few cases, it may never happen.

Also, just as in the larger community, often tenants provide services that are directly responsible for crime and social disorder. Bars, nightclubs, and restaurants sell alcohol to their customers. Unfortunately there will usually be those customers who drink too much and create problems for the larger site, such as causing a variety of disturbances. It will be up to the property management company as a whole to determine what the best course of action is but data for helping to make that decision should be provided by the security department in its regular data collection and analysis. At this point it is important to note that there are unfortunately those property managers and tenants who turn a blind eye to problems generated by tenant activity and use the age old response that "that is why we have security, to deal with these types of problems." As frustrating as this is to hear, security professionals will hear this many times in their career.

Each discrete site will have unique security issues and security issues that all sites have. For example, just about every type of site has theft to deal with. What will be unique to what is being stolen at the site. For a commercial high-rise, it may be laptops being stolen; for a hospital, it may be drugs from the dispensary; for the shopping mall, it will be retail theft. Casino/hotels will deal with theft of employee and visitor property among others. It will be the responsibility of the security professional to determine what is being stolen and then look for potential solutions and communicate these to the retailers. As usual there will be those tenants who have many reasons why a certain security program cannot be instituted, such as it costs too much, losses are the cost of doing business, tenants lack training, they lack head office support, and they want to rely entirely on security to resolve their issue. The security professional needs to be proactive, willing to listen, and overcome these objections with sound and well thought out response, research, data, and facts. They must also recognize some tenants will simply never agree with them. Security professionals must also be willing to document their security program, their tenant contacts, and tenant responses if and when tenants come back after some such incident to counter any accusations of negligence on the part of the security department.

Generally, if security professionals research a particular issue, are knowledgeable and well versed in it, and are reasonable in their interactions with tenants, then most tenants will be more willing to implement a security program when requested. Much of it comes down to credibility and reputation of the security professional making the request.

Tenants, just like so many other assets, have a dual nature. First and foremost, they must be protected and second, they are there to help protect other assets. Providing security is often not the only function of the security department. Security professionals are of the essence to the protection program and that program will very often encompass other potential sources of loss beyond that of the criminal. Occupational health and safety and life safety are two other

areas, particularly life safety where tenant relations are vital to the effectiveness of the site program. For example, in the commercial high-rise, fire wardens are an essential component of the building evacuation plan. Without dozens, if not hundreds, of volunteers, it is difficult, if not impossible, to coordinate a partial or full building evacuation of the thousands of building residents. Cooperation from companies who provide the staff, time for training of those individuals, and equipment are all provided by the tenant. If the companies who lease space in the commercial high-rise think this is a waste of time, then the security manager/supervisor's job will become that much more difficult.

Health and safety is another area where good tenant relations are vital. As already discussed, many discrete sites encompass many hundreds of thousands or millions of square feet. As tenants can generally be found to spread out over much of the facility, the key is to harness the critical mass that can be developed from having hundreds or thousands of individuals spread out across the site to report health and safety violations or potential or actual unsafe work conditions.

It must be stated here that the onsite security manager/supervisor will know his or her site and further will know best how to communicate with his or her tenants. He or she will also know what program is best suited to meet the needs of the individuals and tenants as a whole. What is provided here are merely some suggestions for the security group to consider implementing.

Any site with retailers will benefit from a communication network alerting all who participate in upcoming training, alerts if it is known whether particular shoplifters or shoplifting techniques are being employed, and sharing of photos of suspects (the reader must be cautioned here about privacy laws in effect, they are responsible to determine what they legally can and cannot do in their jurisdiction). Often it is a giant step ahead for tenants and site security to simply meet and get to know each other. Logically what follows is that incident data can be shared to alert others as to what is transpiring on site. One of the greatest challenges at a site is getting tenants to share information between each other. This is where the security manager/supervisor can act as facilitator and information disseminator.

Sites with tenants providing similar services can benefit from regular meetings. This is an excellent opportunity to share similar challenges, whether it is security, life safety, or health and safety related. One benefit will be that additional resources may be freed up. Because similar organizations often operate in silos and feel their problems are unique and no can help them or may feel embarrassed they are experiencing particular issues, thieves are often able to take advantage of this. Instead, when information sharing becomes the norm, tenants can share experiences, learn from each other, share resources, and work in concert to eliminate or reduce threats.

For example, when laptop thefts became a real concern to several property owners and tenants, all parties started cooperating with information sharing related to incidents, how thieves were accessing tenant space, what was stolen, etc. Tenants and the property managers were able to cooperate successfully to the point that targets were hardened to the point thieves were no longer successful in stealing laptops.

What do you do if you suspect your tenant is either involved in criminal activities or more commonly, condoning it? There have been several well-documented examples in housing projects where tenants or employees of property managers have been actively involved in a variety of criminal activities. In four such documented cases, the property management companies, despite repeated requests by local law enforcement, ignored a wide variety of criminal issues until finally forced to act or risk loosing US federal government funding and were also subject to costly fines and criminal charges (Sampson and Scott, 1999, pp. 8–19). This issue is complex and cannot be given full justice but the reader is directed to "Tackling Crime and other Public Safety Problems." A full detail of the material is provided in the "References" section.

If tenants are involved in criminal enterprises, it is the responsibility of any security professional to forward this information on to the appropriate law enforcement officials. It is no different than if security personnel witnessed a crime occurring at the site, when the people involved are visitors. This is obviously a delicate issue and suspicions are not facts.

However, just as the security professional witnesses a crime occurring on the site, and calls local law enforcement, so too should he or she call when observing or suspecting criminal activity on the part of tenants. This is where good relationships with local law enforcement are important. Just as tenants and security personnel, in fact the entire property management group, need to work together, private security and public law enforcement need to have a good working relationship. Just as with tenants, this relationship will take time where lots of two-way communication is necessary.

In many sites, there is often a problem with a wide variety of criminal activities. The fact that there are various services, huge numbers of people, goods for sale, and a variety of assets makes the site attractive from a criminal perspective. This is obviously one of the mandates of the security department. It is not within the scope of this chapter to detail all criminal activity indicators on a site by site specific basis. The security team will know or should know what criminal activities are generated specific to the site. A comprehensive threat and risk assessment is necessary and will help the security manager/supervisor determine what they should be protecting the site from. Furthermore, once this is accomplished, the various security strategies need to be implemented to counter whatever criminal activities are occurring.

When it comes to occupiers' liability, the security manager/supervisor is encouraged to research and determine what the laws are in his or her jurisdiction. Suffice to say, jurisdictions have recognized that owners/occupiers have a duty to protect employees and visitors. This is not just applicable to large discrete sites but to all properties. Over the last several years the courts have ruled in most cases in the victims' favor when they have been on an individual's property. There are a large variety of sources of information relative to this issue with books, magazines, Websites, and newsletters providing considerable detail on this important topic. For example, a recent judicial decision in California stated, "the owners of a bar had a duty to intervene in the attack on a patron" (Anderson, 2005, p. 108). Anthony Marshall, president of the Educational Institute of the American Hotel and Lodging Association states, "By common law, hotels are required to exercise 'reasonable care' for the safety and security of their guests" (de Treville and Longmore-Etheridge, 2004, p. 61). There is no doubt that property owners of discrete sites have a responsibility to protect those who come to their site.

Site Evacuations

A special note needs to be made regarding discrete sites and building evacuations. While there are a variety of issues to be dealt with when it comes to emergency response planning, often the end result is a partial or full site evacuation. In anticipation of that potential, following is a list of points to remember when planning for such an event.

Ten Commandments of Evacuations

1. **They are everyone's responsibility.** A successful evacuation requires everyone's coordination and participation. That means that everyone involved, from the property managers, tenants, and employees, must take responsibility for learning their role.
2. **They are inevitable; therefore, they must be prepared for.** Evacuations, whether they are planned for or not, are going to happen. Most jurisdictions call for annual drills; therefore, even if there are never any incidents requiring an evacuation, the property manager is mandated to conduct at least one drill a year.
3. **They must be regularly practiced.** Employee turnover is a reality. People move on, up, or out, new positions are created, eliminated, or added to. This is true for all parties; therefore, regular practice is an absolute must.
4. **The property manager must lead the training efforts.** Therefore communication between all parties is vital to success. The property manager is in the best position to coordinate training, establish proper procedures, and communicate between all parties; therefore, he or she must lead all efforts in preparing for evacuations.
5. **Senior management from individual companies must buy in and promote the program.** Fire wardens must be supported by their senior management. Taking over

the responsibility of fire warden can be demanding. Training is required for all fire wardens, and regular communication between security and company fire wardens is necessary, supporting the fire warden program.

6. **Local emergency services must be active participants.** Getting local emergency services involved makes sense. In the event of an actual emergency, they would respond; so getting them familiar with the site, developing communication between the on-site security group, and understanding all the parties' roles will allow for a much smoother response.
7. **Fire wardens play a valued role; therefore, they must be robustly encouraged.** Fire wardens are an integral part of the site evacuation process; therefore, they must be supported. The role can be stressful and can at times lead to conflict between coworkers. Helping to evacuate a site with thousands of participants is not always easy. Some people, even in real emergency situations, refuse to evacuate or cooperate with others. This can be a challenge for people to deal with; therefore, support and training from the security manager/supervisor and tenant senior management goes a long way in maintaining the fire warden program.
8. **Partial and full evacuations should be conducted annually.** Most jurisdictions call for mandatory fire drills. As they must be conducted, it makes sense they should be prepared for.
9. **All building management staff must be prepared to help evacuate the site.** The more people who support the evacuation, the better. As many discrete sites are enormous, it only makes sense that all management staff should be involved in the process. The bigger the site, the more people are necessary to help evacuate it.
10. **All management staff must be prepared for and trained to stand in as Incident Coordinator.** As is often the case, emergencies occur when the least amount of staff are on hand to respond to it. They occur on weekends, in the middle of the night, and during holidays. Hence, it should not only be security personnel prepared to step in as incident coordinators but any of the management staff. Training is necessary to prepare people for this responsibility. Again, the more people prepared for an incident, the better it is for all concerned.

Site and building evacuations absolutely rely on good tenant relations. The bottom line is that participating in evacuations is not within the job description of most employees nor is it the mandate of most businesses. They take employees away from doing what they were hired to do, which is to make money for the tenant. They are costly in time, effort, and money. If improperly conducted, they foster mistrust between the tenant base and property owners. Hence, good tenant relations need to be developed and managed for this and many other reasons.

Terrorist Threat Indicators

Terrorist threat indicators, while seemingly not a tenant specific issue, are vital to site protection and do have ramifications for security personnel and tenants. As identified in the six reasons why security should work toward good tenant relations, it is more likely a tenant or visitor will notice suspicious activity sooner than security personnel for no other reason than there are far more tenants out and about a site than there are security staff.

Admittedly, this can be a challenge to present to tenants to be on the lookout for and some property managers may shy away from enlisting the aid of tenants and visitors. However, some sites, depending on what they are, have utilized all visitors to be on the lookout for such activity. In certain countries around the world, everyone is educated in looking for suspicious activity and then forwarding that information onto security or law enforcement.

Their political or religious ideologies and causes may differ, but terrorists share one thing in common—they plan their attacks. This planning produces preoperational indicators that can become apparent in the days, weeks or months prior to an attack. The discovery of one of these indicators may not point to a potential terrorist attack but recognizing clusters of, or linkages between, such factors could lead to preventing one. (Criminal Intelligence Directorate, 2006)

Logistical Support

It encompasses recruitment, training, and equipment acquisition producing the following indicators—often connected to thefts, sales, or seizures:

Research and Training

- Training manuals on the operation of aircrafts, scuba diving, and use of explosives
- Extremist literature or photographs of known terrorists
- Photographs, diagrams, blueprints, maps, or videos of high-profile targets

Documents and Equipment

- Surveillance equipment—cameras, GPS units
- Short wave, two-way radios and scanners
- Multiple cellular phones or prepaid calling cards
- Theft of uniforms (security/military/police) or ID cards/badges

Target Selection

It encompasses surveying potential targets, producing reports of the following incidents:

Site Surveillance

- Multiple sightings of the same person, vehicle, or activity
- Sudden presence of panhandlers, shoe shiners, street vendors
- False alarms requiring emergency responses, with individuals observing procedures
- Damage to perimeter security (breaches in fences)
- Computer hacking attempts to access sites with target data
- Attempts to smuggle contraband into a building

Activities of Individuals

- Making unusual security inquiries
- Photographing security systems, procedures, or guard locations
- Drawing pictures or taking notes
- Using of night vision or thermal devices
- Discrete use of cameras or other observational equipment
- Wearing improper attire for the area or season
- Loitering at bus or train stops or sitting in a parked car for extended periods
- Exhibiting suspicious behavior—staring or quickly looking away from people or vehicles

Nonverbal Suspicious Behaviors

- Lack of eye contact
- Sweating
- Excessive hand movement
- Biting fingernails
- Chewing on the inside of the mouth
- Dry mouth

What to Watch for on Interior Patrol

- People entering a building as a group, then splitting of individually
- Wearing inappropriate attire such as loose or bulky clothing inconsistent with current weather conditions
- Protruding bulges or exposed wires under clothing
- Strange chemical odors
- Mumbling (as in prayers), or unusually calm or detached behavior

- Attempting to gain a position amid a crowd or near an important person
- Tightened hands as if gripping something
- Wearing disguises appropriate to the target area (military, police, fire fighter, or posing a pregnant woman)
- If you see a person acting suspicious or he or she seems to be lost, ask the person if he or she needs any help. If the person is still acting suspicious, notify your supervisor and the command center immediately, so they may get good video of the person
- Watch for a person who wears the backpack on the front, giving access to the interior of the bag
- People asking unusual questions (questions about security procedures, gaining access to restricted areas, how many people are in the building, etc.)
- Watch for people whose body language is aggressive or apprehensive (clenched fists, sweating, praying, etc.)
- Watch for people leaving bags behind
- Watch for tailgaters or piggybackers at turnstiles
- Make sure that visitors have the correct date on their badge
- It is your duty to investigate or challenge a suspicious person or incident, but remember to be polite
- If you have any doubts about a person, notify your supervisor immediately
- Complete an incident report of any suspicious activity and make sure that information is passed along to security/police personnel.

What to Watch for on Exterior Patrol

- When conducting a perimeter patrol, watch the people around you. Example: a person wearing a heavy coat on a warm day, a person behaving suspiciously, a person whose appearance or behavior does not "fit," a person focused on security personnel and equipment
- Unattended vehicles; especially cars, trucks, tankers
- Vehicles that appear to be "overloaded" with heavy cargo
- Vehicles that smell like industrial chemicals (ammonia, gunpowder)
- Vehicles that have "homemade" signage
- Vehicles that are leaking fuel, chemicals, or having wires hanging from them
- Unattended packages, backpacks, boxes
- Check the planter boxes and garbage cans; anyplace a device could be hidden by someone walking by
- Check the exterior doors
- Look up at the building to make sure no one is placing an object next to it or climbing the walls
- Do not be afraid to investigate further or to ask questions
- If something does not look right, contact your supervisor immediately

Command Centre

- Stay alert during camera patrols
- If you see any suspicious people or behavior, investigate further and notify the supervisor immediately
- Try to get clear video shots of people or vehicles associated with suspicious behavior (faces, license plates, etc.)
- Watch for people who appear to be "watching" us
- Watch for people who are taking pictures of restricted areas and security equipment, sketching drawings, or making notes
- When in the command centre, move the cameras around at different time intervals; do not get into the "every two hours" rut
- Monitor the cameras in the freight lobbies and elevators
- Pay special attention to access control alarms in restricted areas

This chapter has introduced the reader to how tenant relations, both good and bad, impact the security professional's site protection of asset's plan. The proactive security manager/supervisor will take advantage of the benefits accorded by good tenant relations. Every discrete site has unique characteristics separating it from any other site. Having said that, there are many commonalities shared by most discrete sites. It will be up to the security managers/supervisors to best determine what will work for them.

References

T. Anderson (2005). Legal report: US judicial decisions. *Security Management* 49(12): 108–110.

P. L. Bennett (Fall 2006). Evacuation planning: Four mistakes managers make. *Disaster Resource Guide for Facilities* 11(2): 24–26.

N. Christie (1994). *Crime Control as Industry*. 2nd Edition, New York: Routledge.

Criminal Intelligence Directorate (2006). *Terrorist Threat Indicators Pamphlet*. Ottawa: RCMP.

R. H. de Treville and A. Longmore-Etheridge (2004). Time to check out liability trends. *Security Management* 48(2): 61–65.

B. George, and M. Button (2000). *Private Security*. Leicester: Perpetuity Press.

Introduction to Security and Crime Risk Management, Module 1, University Leicester, England, 1999.

http://www.cops.usdoj.gov/Default.asp?Item = 36, accessed October 22, 2006.

http://en.wikipedia.org/wiki/West_Edmonton_Mall, accessed November 11, 2006.

L. Johnston (1992). *The Rebirth of Private Policing*. London: Routledge.

Dr. G. Marquis (2000). Social contract/private contract: the evolution of policing and private security. In *Police and Private Security: What the Future Holds*, ed. J. Richardson, Ottawa: Canadian Association of Chiefs of Police.

R. Minion, and S. Davies, *Protection Officer Training Manual,* 7th Edition, Butterworth-Heinemann, 2003.

C. Murphy and C. Clarke (2005). Policing communities and communities of policing: A comparative study of policing and security in two Canadian communities. In *Re-Imagining Policing in Canada*, ed. D. Cooley, Toronto: University of Toronto Press.

J. F. Pastor (2003). *The Privatization of Police in America*. Jefferson: McFarland.

Portland: Wellan Publishing.

Protect: Privatization and Community in Criminal Justice. New York: New York University Press.

R. Sampson, and M. S. Scott (1999). *Tackling Crime and other Public Safety Problems: Case Studies in Problem Solving*. A COPS Publication: US Department of Justice.

T. Sandors (January 2005). Rise of the rent-a-cop: Private security in Canada, 1991–2001. In *Canadian Journal of Criminology and Criminal Justice*, ed. P. Carrington, vol. 47(1). Toronto: University of Toronto Press.

Tenant Relations

Quiz

1. "_____ crime prevention" focuses on the specifics of the crime, whereas "_____ crime prevention" focus on the root causes of crime. Both social and environmental crime prevention impact and, in turn, are impacted by security professionals

2. Just as police recognize the value of engaging the community in crime prevention strategies, so too should security professionals be willing to engage the _____ site community in the same strategies.

3. One definition of a discrete site is a "predefined area/structure with unique characteristics that differentiate it from surroundings." ☐ T ☐ F

4. One such loss prevention model is the WAECUP acronym. It stands for **W**aste, **A**ccidents, **E**rrors, **C**rime and **U**nacceptable **P**ractices. ☐ T ☐ F

5. The tenant security program focuses on crime and environmental and social disorder through the delivery of security services that include aspects of traditional protection strategies, as well as _____, _____, _____, and _____. The tenant security model balances reactive responses to calls for service with proactive problem-solving centered on the causes of crime and disorder.

6. As tenants can generally be found to spread out over much of the facility, the key is to harness the critical mass that can be developed from having hundreds or thousands of individuals spread out across the site to report health and safety violations or potential or actual unsafe work conditions. ☐ T ☐ F

7. When it comes to _____, security managers/supervisors is encouraged to research and determine what the laws are in their jurisdiction.

8. Site and building evacuations absolutely rely on good tenant relations. They are costly in time, effort, and money. If improperly conducted, they foster mistrust between the tenant base and property owners. Hence, good tenant relations need to be developed and managed for this and many other reasons. ☐ T ☐ F

9. While there are a variety of issues to be dealt with when it comes to emergency response planning, rarely the end result is a partial or full site evacuation. ☐ T ☐ F

10. _____, while seemingly not a tenant-specific issue, are vital to site protection and do have ramifications for security personnel and tenants. As identified in the six reasons why security should work toward good tenant relations, it is more likely a tenant or visitor will notice suspicious activity sooner than security personnel for no other reason than there are far more tenants out and about a site than there are security staff.

This page intentionally left blank

4

Uniforms and Image Projection for Protection Forces

Megan Bupp and Matthew Bietsch

Role of the Security Officer

Uniforms demonstrate consistency and authority within an organization. Security/protection officers are often the first people that visitors to an enterprise encounter; therefore, employers see the need for their officers to be professionally attired. However, protection officers should not rely only on their uniform to maintain a professional image; they must also ensure that every facet of their being serves to project a positive public image, including their demeanor and the manner in which they interact with people.

Uniforms not only allow a protection officer to obtain the respect of the community but also provide a foundation for a protection officer's self-respect. According to Sennewald (1985, p. 66), "Issuing or permitting the use of shabby uniforms.… takes away from a man's sense of pride. High standards for uniforms, on the other hand, automatically instill self-pride, and hence, self-respect."

History

Prior to the Second World War, security officer uniforms were not a concern because, in Brennan's words (1985), "there were not security guard forces. Security, where it existed at all, was provided by night watchmen making clock rounds with a flashlight.… Since no one else was in the building during his shift, the night watchmen dressed for his own comfort, according to the circumstances of his location.

However, in policing, the projection of an impressive image through uniforms can be traced back to a statement made by Sir Robert Peel, the Father of Modern Policing, while he was reforming the London Metropolitan Police Department in the 1800s—according to Betterton (2003), Peel was quoted as stating that "good appearance commands respect.

The Effect of Uniform Color

In their article "Dimensions of uniform perceptions among service providers," Daniel *et al*. (1996) cite a study done by Frank and Gilovich (1985) that outlined the impact that ice hockey uniform color had on players' actions and on referees' and spectators' perceptions of the players. The researchers concluded that "color was particularly salient in domains that were already in possession of competition, confrontation and physical aggression. In the article, Daniel *et al*. highlight the negative impact that the researchers found that black ice hockey uniforms had on spectators, umpires, and wearers:

- *black uniforms were perceived by spectators to look more malevolent, more active, and strong than nonblack uniforms;*

- *black uniform teams were more likely to have earned high penalties, either as a result of more aggressive play or the perception of aggressiveness on the part of the referee;*
- *black uniform teams did receive harsher penalties from umpires;*
- *wearing a black uniform induced subjects to choose more aggressive games and to express more aggressive thoughts.*

Although this study was done in relation to ice hockey uniforms, the results may be applicable to public perception of law enforcement uniform colors as well. For example, out of 12 survey responses by police/sheriff's departments in a study of uniform colors done by Martin (2001), 9 departments indicated that they had recently changed uniform colors, but only 5 of the nine departments "stated there was a positive change in public perception of the officers" after the color change (3). Perhaps this is because 8 of the 9 departments changed their uniform color to dark blue for both the shirts and pants (from either tan/tan, gray/blue, dark blue/light blue, tan/blue, or dark brown/tan), and dark blue is very similar to black.

Daniel includes other examples of the connotations associated with various uniform colors (as reported in a 1993 study by Rafaeli and Pratt)—"blue represented authority and dignity on the part of the wearer and the organization they represented, while pink associated the wearer with femininity and the organization with a feminine-oriented service.

Sennewald describes a program implemented in Broadway Department Stores in which the design of store detectives' uniforms, combined with the detectives' increased visible presence throughout the store, proved effective in deterring shoplifting. About 80% of the store detective staff was retrained to "prevent shoplifting by being highly visible (wearing a tailored red sport coat with a gold cloth pocket badge reading 'Security') and constantly moving about the store with a pleasant expression on their face making eye contact with as many customers as possible" in order to discourage theft (Sennewald and Christman, 2007). The remaining 20% of the store detectives retained their plainclothes approach to preventing shoplifting in order to detect those would-be shoplifters who were not deterred by the presence of the Red Coats. In the words of Sennewald, "It was a balancing act that worked." Here, we see that red was an effective choice for uniform color because red blazers, in conjunction with a pleasant and professional attitude on the part of the store detectives, served to project a highly visible and effective security image that successfully deterred crime.

Uniform Styles

According to Brennan (1985), "security officers agree that properly designed and properly worn uniforms achieve three basic goals: enhanced image for the employer, enhanced self-image of the guard, and enhanced security for the company. In terms of enhanced image for the employer, "The message conveyed by a professional guard presence is that of a company that takes itself, its business, and its customers seriously. Any customer will appreciate this attitude. Furthermore, "Security guards who look good usually feel good about themselves and their job. As a result, guards do their job better. In addition to eliciting a positive image for the employer and a positive self-image for officers, professionally attired guards serve as a deterrent to crime. Brennan quotes James Dunbar, CPP, president of the Loughlin Security Agency in Baltimore, MD, as stating that "This is where we [contract guard companies] provide our greatest service to customers—crimes that never happened because one of our guards was on the scene, looking and acting in a professional manner.

Brennan discusses uniforms as falling into one of three categories: the "military look," the "security officer look," and the "soft look." The standard military look uniform "comes with a traditional eight-point police cap or round military cap, a navy blue blouse coat with matching pants, a white shirt, dark tie and black shoes. This type of uniform is most often utilized by municipalities and by larger companies who employ private security officers. Brennan states that although this type of uniform projects a very professional image, it may be "bulky and cumbersome. Additionally, he warns that companies who use this type of uniform should not copy local police uniforms too closely, especially since some municipalities expressly forbid security officers from wearing uniforms that are similar to those worn by the police. For instance, a provision of the Oakland (California) Municipal Code for Private Patrol Services and Private Watchman clearly states that it is

unlawful for the uniforms of private watchmen and private security officers to be similar in design to any uniform worn by Oakland police officers or firefighters (private watchmen and security officers should not be mistaken for police or firefighters because of the appearance of their uniforms).

Brennan deems the military look best suited for "stationary guard positions where a highly visible security presence is desired.

The "soft look" in uniforms is usually employed in indoor posts where a harder look may not be appropriate (such as in hotels, casinos, hospitals, and in corporate offices) and this uniform style typically consists of blue blazers with blue or gray slacks. Brennan feels that the main advantage of this look is that it allows establishments to provide a nonintimidating approach to security. One possible drawback to this look is the need to carry personal protective equipment, cell phone, radio, handcuffs, etc. Having all this on an officer's belt is cumbersome. This makes the wearing of business attire difficult.

The "security officer look" in uniforms falls in between the styles of the military look uniform and the soft look uniform. According to Brennan, "Proponents of the security officer look maintain that guard uniforms can be clearly different from local police uniforms without sacrificing the deterrence value of the military style. This uniform style "stresses materials and styles that are functional, durable and easy to maintain. Emphasis is on shorter jackets, minimal decoration, and lightweight, water-repellent material such as 100 percent texturized knits and dacron/cotton permanent press fabrics.

Costello (2001) constructed and implemented a survey designed to discover why security officer uniforms differ so greatly between health care organizations (a police- or military-style uniform versus a blazer and slacks versus casual/business clothes). The survey was distributed to various health care organizations across the country.

The results of this survey indicated that the majority of the organizations questioned outfitted their security officers in a police- or military-style uniform. For most, these uniforms were chosen because security directors view the uniforms as crime deterrents and because they feel that the uniforms make the officers more easily identifiable in an emergency situation. Additionally, an overwhelming majority of these respondents indicated that their security officer uniforms were the same color as their local police department uniforms. In essence, this survey demonstrates that when crime is a factor in a facility, security directors prefer to outfit their guards in clothing similar to that of the police because these uniforms act as a crime deterrent and make their officers more easily identifiable.

Those organizations who choose to outfit their officers in a blazer and slacks indicated that they do so because of the emphasis that they place on the public relations aspect of a security presence; therefore, these organizations strive to keep the security officer's profile low key.

Costello himself voices his agreement with the outfitting of officers in police-style uniforms. He states that one of the major responsibilities of a security officer is to prevent crime, and through experience, he or she has seen this facet of the job better accomplished with this type of uniform. However, as discussed previously, some debate has arisen regarding security officers wearing police-style uniforms. There is also a need for more research in this area although crime deterrence is difficult to measure.

Uniform Materials and Appearance

Officers are expected to keep uniforms, insignia, accessories, all issued equipment, and all authorized personal equipment clean and in good repair at all times. The following is a sample dress code that illustrates the level of significance that some employers place on their employees' attire:

1. Long sleeved shirts may be worn as outer garments or under an agency-issued or -approved jacket. Long sleeved shirts will be buttoned at the cuff. A shirt may be professionally altered for proper fit. (This does not apply to the BDU jacket.)
2. Trouser legs are to be uncuffed and hemmed at the point where they touch the shoe tops without causing a break in the crease line, or they may be altered with a slight break in the crease line for proper fit.

3. Issued/approved jackets may be worn during cold weather or other inclement conditions.
4. Only black socks are to be worn, and they must be long enough so that skin will not show below the trouser cuffs when walking or sitting.
5. Footwear must be properly shined and in good condition. Shoes/boots must be black in color with black laces and plain toe. Black sneakers are not acceptable footwear.
6. Uniforms are to be kept clean and neatly pressed at all times. This includes shirts, trousers, blouses, skirts, jackets, and any outer garment that is a part of your uniform.
7. Uniform hat or cap, if worn, will be placed squarely on the head and will not tilt to the sides or the back, or be worn backwards.
8. The tie will be clean.
9. All badges will be clean and shined and worn over the left breast pocket of the uniform shirt or jacket.
10. Shoulder patches will be worn on the left and right shoulders of the shirt, overcoat, or jacket, sewn into place, and centered approximately 1 in. from the top of the shoulder patch.
11. The nameplate may be of metal or plastic material and silver in color, with 1/4-in. black printed lettering with the officer's last name. If desirable and appropriate, the officer's first initial may be imprinted. The nameplate shall be centered above the right pocket, and flush to the top of the pocket.
12. Officers may wear only the accessories that they are qualified or authorized to wear. If awards are to be worn, they should be placed 1/8 in. above the nameplate. If only one award in worn, center it above the nameplate; if more than one award is worn, center to the top of the pocket, 1/8 in. above the nametag, in order of precedence.

Betterton (2004) provides a basic approach to inspecting and maintaining uniforms. He suggests a uniform inspection be conducted in the following manner: place the uniform shirts and trousers on separate hangers at eye level and look over them closely, checking for "those nasty loose threads also known as 'Irish pendants'—loose or missing buttons, stains or spots, discoloration, [and] extensive wear or damage. In regards to the uniform shirt, pay close attention to the collar, shoulder seams, pocket flaps, and button holes and check for and cut off any loose threads. With the uniform trousers, carefully check all pockets. Again, cut off any loose threads and, in the words of Betterton, "Remember anything placed in the pockets creates a wear mark and wear marks make a uniform non-serviceable. Ditch the car keys, coins, wallets, cosmetics and the good old snuff can. After checking the shirts and trousers individually, look closely at the pressed creases and make sure that they are crisp and where they are supposed to be—"Take a few minutes and touch them up with an iron should they need it. Nothing looks worse than double creases.

Bellah (2002) discusses trends in uniform manufacturing and provides information about various types of materials commonly used in the manufacturing of uniforms, including wool, cotton, polyester, and fabric blends. According to Bellah, wool "projects a professional appearance, will retain its color against repeated cleanings and Ultra-Violet exposure over a long period of time, and it breathes. Additionally, wool has natural fire-retardant properties and therefore will not melt when exposed to flame and heat. However, wool is expensive to manufacture and will cause discomfort in hot, humid regions. Wool must be dry cleaned and if it is not cleaned correctly, it will shrink after exposure to water.

Cotton is a material that is well suited for use in warm, dry areas. It is lightweight and, unlike wool, is washable and inexpensive to manufacture. However, it "wrinkles easily, lacks durability and will fade after repeated washings and UV exposure. Another downside of cotton is that it is very absorbent and will take a long time to dry after becoming wet.

Polyester is a strong, durable, wrinkle-resistant wash and wear fabric that will retain its color after repeated washing and ultraviolet exposure. Like wool, 100% polyester garments can be uncomfortable in hot, humid regions. A main concern with polyester is that it is not fire retardant and it will melt when exposed to flame.

Fabric blends "have been around for several years, and the latest advancements allow blends of natural and synthetic fabrics so the uniform can be tailored to allow the maximum

comfort, wear and colorfast properties and affords officer safety" (Bellah, 2002). Bellah provides three examples of fabric blends—Gore-Tex®, Crosstech®, and Nomex®. Gore-Tex® is a fabric developed by W. L. Gore & Associates that provides the advantages of being water- and wind-proof, yet allowing for the release of sweat vapors. Crosstech® is also manufactured by W. L. Gore & Associates and is similar to Gore-Tex®. Crosstech® provides protection against blood-borne pathogens and common hazardous chemicals (such as DEET insect repellent, gasoline, battery acid, and fire-fighting foam). Nomex® is manufactured by DuPont® and it allows for superior flame and heat resistance. According to Bellah, "Nomex® and other fire resistant fabrics such as Kermel® have been blended with other fabrics to make fire resistant garments.

The type of uniform worn by security officers can vary depending on the climate of the portion of the country in which they are employed and also on the environment in which they work. A debate arose between the National Treasury Employees Union and the Department of Homeland Security, Border and Transportation Security Directorate, Bureau of Customs and Border Protection regarding the nature of employee uniforms; specifically, whether Customs Inspectors and Canine Enforcement Officers should be allowed to wear uniform cargo shorts. Many of these officers are required to work in hot, humid weather conditions and to work inside aircraft cargo compartments with the temperatures in excess of 100 F. The employer argued that these shorts do not project a professional image, to which the Union responded that during the 5 years that these shorts have been worn, there have been no known complaints. The employer requested that cargo shorts be worn only by those officers stationed in South Florida, Puerto Rico, and along the Southwest border, for the above-stated reason and because CPB employees come into contact with a number of hazardous substances with the potential to damage the skin.

The Role of Uniforms in Inspecting and Briefing the Shift

Prior to the beginning of the shift, personnel should be inspected and instructed. This preshift inspection is effective for several reasons:

1. It keeps employees informed of management goals and the steps being taken to achieve them, thereby helping to maintain security personnel as members of the management team.
2. It ensures that each employee has been instructed in current job information. This information may change from day to day.
3. It ensures a free exchange of ideas, which helps foster creative thinking as well as minimize potential problems.
4. It provides supervisors with a means of inspecting personnel prior to their being assigned duties. This can preclude problems of a serious nature later on.

In regard to personal appearance and uniform inspections, supervisors should keep in mind that "A professional image is crucial to the success of any security officer"; this is especially true for those officers who interact with the public. Officers whose appearance is substandard should not be permitted to man posts. (Preventing unkempt officers from manning posts is a policy that allows an organization to uphold its professional image and to avoid public comments regarding an unkempt officer's appearance.)

Uniforms should be worn and maintained in accordance with company policy at all times—an officer in an improper uniform causes the organization to suffer a drop in prestige. The officer himself will suffer from disciplinary actions.

Conclusion

A well-maintained uniform can serve to enhance a security officer's presence and can therefore allow the officer to better serve his or her organization. Investing in high quality, durable uniforms that project a professional presence is in keeping with the precepts of proactive management. Ensuring that officers look their best is the shared responsibility of both first line supervisors and the officers themselves.

References

J. Bellah (Oct. 2002). What's new in uniforms. *Law & Order* 50(10). Retrieved November 1, 2006 from ProQuest article database.
K. Betterton (May 2004). Uniform preparation and maintenance. *Law & Order* 52(5). Retrieved February 5, 2005 from ProQuest article database.
K. Betterton (Sep. 2003). Basic principles for high quality uniform appearance: It's easier than you think. *Law & Order* 51(9). Retrieved February 5, 2005 from ProQuest article database.
J. Brennan (1985). Outfitting your guard force. *The Protection Officer* 2(3):14–15, 29–30.
J. Costello (Nov. 2001). Uniform appearances. *Protection Officer News*. Retrieved October 21, 2006 from http://ifpo.org/articlebank/uniform_appearance.html
K. Daniel, L. W. Johnson, and K. E. Miller (1996). Dimensions of uniform perceptions among service providers. *The Journal of Services Marketing* 10(2):42–56.
C. Sennewald (1985). *Effective Security Management: Second Edition*. Boston, MA: Butterworth Publishers.
C. Sennewald, and J. Christman (2007). *Retail Crime, Security & Loss Prevention: An Encyclopedic Reference*. Burlington, MA: Butterworth-Heinemann.

Uniforms and Image Projection for Protection Forces

Quiz

1. True/False—Before the First World War, security officer uniforms were not a necessity because security guard forces did not exist.
2. Which historical figure made the statement "good appearance commands respect"?
   a. Edward Sutherland
   b. Robert Peel
   c. J. Edgar Hoover
   d. Allan Pinkerton
3. Studies have shown which of the following uniform colors often has a negative effect on the wearer and on those who come into contact with the wearer:
   a. black
   b. white
   c. navy
   d. brown
4. True/False—The Broadway Department Stores program that stressed a highly visible security presence outfitted security officers in a tailored red sport coat with a gold cloth pocket badge reading "Security."
5. Name the three basic goals that properly designed and properly worn uniforms achieve.
6. Name Brennan's three categories of uniforms.
7. The results of Costello's survey indicated that most organizations outfit their security forces in which type of uniforms:
   a. a blazer and slacks
   b. police- or military-style
   c. casual/business clothes
   d. none of the above
8. The military look in uniforms is best suited for officers who routinely patrol an organization's premises.
9. True/False—When inspecting a uniform, one should place the shirts and trousers on the bed (or other flat surface) and look down at them.
10. Name three advantages of using the fabric blend Gore-Tex® in the construction of uniforms.

5

The Relationship Between Marketing and the Security Function

Benn H. Ramnarine
Ramdayal K. Ramdeen
Christopher A. Hertig and
Jimmy Wilson

Introduction

History teaches us that marketing precedes protection in many instances. Organizations hope to gain a profit and fail to see the potential for loss in doing so. It may be said that marketing "trumps" security in that marketing efforts are undertaken in hopes of gaining a profit before any protective concerns are addressed. Banks put up ATMs to reach customers before thinking of the crime risks these posed. Many organizations established Web sites without considering the crime loss consequences.

Marketing is closely related to "quality-of-life" issues. This has become a major part of contemporary urban planning insofar as public policing is concerned. As cities strive to develop a tourist trade, they must eliminate the appearances of crime and disorder. They must drive the homeless off the streets where they may be seen by members of the public. The "broken windows" concept can be thought of as part of a marketing campaign.

Security or police officers are often the first persons seen by visitors to a facility. They may also be the last representative of the organization seen. Protection officers respond to a host of visitor inquiries and requests for assistance. A substantial number of these are outside the realm of protection.

"Exclusivity" is part of marketing. Facilities are more attractive to some clients due to their exclusive nature. The protection organization is then charged with controlling access to the property in a manner that is consistent with customer/user expectations. Exclusive resorts, hotels, country clubs, and gated communities all exhibit some degree of "exclusivity."

Crime Prevention Through Environmental Design (CPTED) may be the theory most closely tying marketing to protection. CPTED emphasizes a natural blending in of protection so that it is unobtrusive. This is in stark contrast to a traditional physical security approach whereby assets/facilities are hardened with little thought given to aesthetics.

CPTED also is arguably more cost-effective than traditional physical security approaches. Security is blended into the environment in such a manner that protection is obtained simultaneously with other benefits. Placing a security office between floors in a parking garage creates greater natural and organized (patrols by officers) surveillance for the parking area. It also may lower response time and reduce the distance that officers must travel on patrol. A further cost saving may be that the space is readily available and already has a floor and roof. A jogging path around a college campus or walking paths for dog owners around a park enhance natural surveillance. At the same time these features provide for recreational usage of the property.

The strategic employment of lighting is perhaps the most obvious evidence of a marriage between marketing and security. Lighting makes property and people look more appealing. While added light provides some deterrent to criminal/unauthorized activity, it also enhances safety. More in line with marketing, it helps to promote a positive image of an environment or object. An example of the latter would be a display in a retail store.

Lighting relates to the WAECUP Model in that it aids in reducing loss due to Accident, Error, Crime, and Unethical/Unprofessional Practices.

Lighting also aids in maintaining greater safety, increasing efficiency, or productivity. It helps ensure that the organization is in compliance with lighting standards and laws.

By incorporating marketing in protection designs, there is a greater bundling of return on design investments. What makes for better security (protection from the malevolent acts of humans) also enhances safety, productivity/efficiency, standard compliance, and marketing.

The techniques used in advertising are amenable to cultivating the desired image of the protection organization. This is important as gaining the willing cooperation of those being protected is essential for daily and emergency operations. It is vital to investigative efforts that persons be willing to approach members of the protection organization (Loss Prevention Department, Security Department, or contract firm) with information on suspicious circumstances.

While the discussion that follows is oriented toward those who provide security services to external clients, the astute protection professional understands that in-house security organizations also provide services to clients: upper management, other departments, or in some cases, external organizations. Whether employed by a contract agency or a proprietary organization, the security supervisor or manager needs to relate to an end user. In some cases there may be more than one end user, such as when third parties (visitors, tenants, guests, patrons, etc.) derive some benefit from the security service provided. Moreover, one must see the competition—both in present and in future—in order to survive and thrive professionally.

The increasingly competitive security service markets of today are leading to a change in attitude toward marketing concepts in the security industry. More and more security organizations are taking marketing seriously and are seeking to attain a professional stand in their marketing drive. Similarly, security service firms are taking service provision more seriously. Quality selection and training of personnel is becoming increasingly common.

Security Market Needs

As security markets grow and services become diverse, the competitiveness of the industry will force organizations to conduct assessments of themselves and consider the following:

a) Their understanding of their client/customer's needs
b) Client/customer's attitudes
c) Client/customer's buying power and behavior

The security organization will need to package its services and gear the corporate image to become competitively attractive.

The Concept of Services Marketing

Services' marketing has increased in importance over the past two decades with the resultant increase in competition. The question of what constitutes a service has to be explored with a view to providing the precise service:

> *A Service is an activity which has some element of intangibility associated with it, which involves some interaction with customers or with property in their possession and does not result in a transfer of ownership. A change in condition may occur and production of the service may or may not be closely associated with a physical product. (Adrian Payne, The Essence of Services Marketing, Prentice Hall International (U.K.) Ltd. 1993)*

The question of what constitutes a "product" in the security service is rather vague. Terms such as "product," "service," or "product service" may be used quite loosely to indicate the same service.

In an effort to market the security product, one should not be too concerned with a definition per se but rather with the "requirements" of the client/end user and what the security organization "offers" to its customers.

Security Services Marketing

Persons involved in security services marketing are dealing basically with an intangible product versus security equipment and supplies that tend to have tangible characteristics. Security services cannot be produced before they are required and stored to meet a demand (for example, a bottle of detergent). The service is therefore most likely "used up" while it is being performed and invariably the consumer of the service is actually involved in its consumption.

The main difference between goods and services in the industry is that the services offered by the security service are "performed" whereas the foods are "produced." The service, therefore, is physically intangible and cannot be seen, heard, smelled, tasted, or touched.

Security services' marketing therefore has a variety of unique challenges for security administration or the company:

1. How can security achieve a unique corporate image?
2. How to offer a service differentiation?
3. How to achieve a distinctive reputation in the marketplace?

In a competitive market, your security marketing skills must be precise and clear in order to satisfactorily market services and liaise with the client.

Selling the Security Service

"Selling is the art of developing relationships." For the security practitioner, this includes practicing qualities consistent for selling the services, which includes the following:

1. Acting with integrity
2. Honesty
3. Professionalism
4. Commitment
5. Customer relations
6. Trustworthiness
7. Market oriented

All these qualities are translated into consultive behaviors. The security supervisor should

1. Learn about consultive behavior
2. Become knowledgeable about the customer's business
3. Become excellent listeners
4. Become excellent communicators
5. Understand the customer's customer

Having achieved this, the security supervisor then becomes a clearing house of information leading from the customer's organization back to the security company. The security company will then be in a position to deal with these definite possibilities:

1. Recognize new opportunities within the customer's identified needs.
2. Handle potential and/or problems early.
3. Become highly effective in preparing and delivering services to the customer.
   Contingency planning is very important here.

The security supervisor who operates as an effective consulting/marketing person obtains substantially more information quickly and currently. Information of this calibre serves the security company in a variety of ways:

1. It allows the organization to assess its quality and strength.
2. It allows for measured performance.
3. It allows for improved strategic planning.
4. It allows for faster effective decisions.
5. It determines where to target for measured efforts.
6. It allows the company to hold and maintain that competitive edge.

Each security supervisor involved in the selling of services, skills, and behaviors should use one's knowledge of the customer's business to identify the customer's business problems, potential problems, and solutions for increased business and security effectiveness.

Mission Statement

The development of a mission statement is most important in services marketing given the intangibility of the security service. Companies/organizations need to develop a clear "mission," a statement of performance to ensure that adequate planning and supervision is directed toward achieving those critical elements of the strategic plan.

While organizations prepare mission statements for a variety of reasons, they should reflect elements of the strategies of the organization and focus on the organization's business activities. Specifically, it should outline a long-term plan of the company indicating what it wants to be and the direction it plans to take. The mission statement is an absolute mechanism for developing and reviewing the strategic market and service options of the security department.

Service-Oriented Mission Statement

It is particularly important in the security industry to avoid a mission statement that reflects "product" rather than "service." The mission should be defined in a way to reflect customer needs rather than product features. "Service needs" should be of major concern for the security director when making a decision about the nature of what services they will offer. Such a statement should contain some of the following components:

a) Who are the customers?
b) Range and type of services—the diversity of services offered
c) Market—where does the security service compete?
d) Long- and short-term objectives—immediate action plan, long-term action plan
e) The organization as a good corporate citizen—concern for the security service's public image
f) Employee satisfaction—the employer's attitude toward the security officer and client
g) Marketing strategies—value, plans, and projections to capture market segment
h) Total Quality Service

The Customer—Security Service Interface

The security supervisor has a responsibility to sell services personally. In doing so, he or she has to consider the following:

1. Personal contact and relationship between the security department and the customer.
2. Development and training in marketing and total quality service.
3. Service is the product and it must be quality oriented.

The relationship between the customer and the security supervisor must be an ongoing relationship. He or she can sell the services through:

1. Good communication skills
2. Sales planning
3. Handling conflict/negative input
4. Analysis of target market
5. Good negotiation of agreement(s)

The Security Interface must Include

1. Personal contact—Client/customer should be managed through personal contact.
2. Customer/security satisfaction—intimate and professional contact provides the basics for the relationship between customer and security.
3. The security supervisor is the first-line marketing officer. He or she acts as the first-line sales person because of positioning to communicate details of services to
   a) Clients
   b) Customers
   c) Potential customers
   d) Advertising agencies
   e) Security publications

The Security Survey

The security supervisor's interface will also come into play in conducting security surveys. This enables the supervisor to ascertain the security status and identification of deficiencies or other vulnerabilities of a potential client. The survey is important as it gives the supervisor his "mechanism" to determine clients' needs. While the survey serves to provide an objective insight into the security needs of a customer, it can also be used to market security services to current customers and future potential ones.

The Responsibilities of the Supervisor in Conducting Security Surveys

The supervisor should conduct the survey as part of his or her initial marketing plan. Here are some suggested guidelines:

1. Goals and objectives should be clear and upper management must support the survey effort.
2. Identify the time, support, and availability of other resources that can be of assistance.
3. Conduct research on the history and background of the location or facility, including geographical location.
4. Check the interactions the location or facility has with the community and clients.
5. Check the crime situation in the area and consider using a commercial database such as CAP Index.
6. Compile internal loss statistics.
7. Assess relevant legal standards and guidelines.
8. Review policies, rules, regulations, and standard operating procedure.
9. Check plans, other architectural drawings, and previous surveys.
10. Compile a list of services that can be provided to the client in order of priority, this excludes the original requirements identified by the client.
11. Compile the survey report—excluding the list of potential services.
12. The list of services to the client should reflect a cost-effective approach or a bundled deal.

There is no set method for marketing the identified services; however, the supervisor must be aware of costs and what the competition is like. The final presentation to the client should be

1. Clear
2. Well prepared
3. Customer oriented
4. Confident in approach and presentation
5. Organized with total quality service in mind and nothing should be left to chance

Summary

Services' marketing provides that competitive edge for many a company. The effectiveness of it is dependent on companies recognizing the differences between the marketing activity and the process to achieve it. The security supervisor's continuous contact with the customer and reaction to research, planning, selling, advertising, and interfacing with the entire security organization, regarding customer needs and requests, will cause a cross-fertilization of activities to emerge. This will further serve to enhance a total quality service package depending on whether the security company has a total quality management system.

The supervisor must also be aware that in striving to market his security services, the training and development of staff is essential. It must not be thought that higher quality means higher cost, for it is more of building quality into services, preventing failures from occurring and eliminating financial waste. Personnel are the key to your quality service becoming a success.

Services will emerge through the provision of quality service. In striving to provide a "top-notch" service to client/customer, communicate as you never have before, involve management in leading roles, measure for success, train like crazy, and give recognition where it is deserved.

Services will emerge through the provision of quality service and reliability. The entire company has to become involved in providing that "top-notch" security service.

The Ten Commandments of Marketing

I. A positive image is always reflected in the bottom line.
II. Target markets must be identified in terms of customer profiles (demographics, buying motives, and buying patterns).
III. Quality is defined by the customer, *not* by the producer.
IV. Pricing must be determined in terms of costs and market conditions in order to be attractive to the customer.
V. "People only buy something after they hear about it 3 times."
VI. Negative customer service is the most powerful advertising tool.
VII. Visualization of the product or service via charts, graphs, etc. is important to influencing buying decisions as is documentation where facts and figures are offered as evidence of product/service worthiness.
VIII. Association of the product or service with something noteworthy or appealing to the target market helps to sell it.
IX. Physical representation via logo or trademark helps establish a product/service identity.
X. Market development—the exploration of new markets—should occur in order to keep the product/service in demand.

Bibliography

J. Bateson (1984). *Managing Services Marketing*. Dryden, Chicago: Text and Readings.,
D. Cowell. (1984). *The Marketing of Services*. London: Heinemann.

P. Connolly, and C. Wilson (1992). *The Survey of Quality Values in Practice*. Clark Wilson Publishing Company.
J. M. Rathmell (1974). *Marketing in the Service Sector*. Cambridge, MA: Winthrop Publishing.
D. L. Riddle (1986). *Service-Led Growth*. New York: Pradger.
Mike Robson (1984). *Quality Circles-A Practical Guide*. Aldershot, Hants, England: Gower Publishing Company Ltd.
P. L. Towsend (1986). *Commit to Quality*, Chichester: Wiley.
A. Wilson (1984). *Practice Development for Professional Firms*. London: McGraw Hill.

Periodicals

Supervisor Management, Publisher: American Management Association, P.O. Box 58155, Boulder, CO. 8033–8155, U.S.A.
Management Review, Publisher: American Management Association AMA Publications, Box 408, Saranac Lake, NY 12983–0408, U.S.A.
International Management, Publisher: Reed Business Publishing, Quadrant House, The Quadrant, Sutton, Surrey, SMZ 5AS, U.K.
International Journal of Strategic Management, Publisher: Pargamon Press Inc., 660 White Plains Road, Tarrydown, NY 10591–5153, U.S.A.
International Business Week, Publisher: McGraw Hill Inc., 1221 Avenue of the Americas, New York, NY 10020, U.S.A.
International Security Review, Publisher: FMJ International Publishers Ltd., Queensway House, 2 Queensway, Redhill, Surrey RH2 1QS, U.K.
Public Relations Quarterly, Publisher: Public Relations Quarterly, 44 West Market St., Rhineback, NY 12572, 914–876–2081, U.S.A.
Security, Publisher: Cahners Publishing Company, Div. of Reed Publishing Company U.S.A., 275 Washington St., Newton, MA 2158–1630, U.S.A.

Marketing the Security Function

Quiz

1. Services marketing has increased in importance over the past decade with resultant increase in _____.
2. The main difference between goods and services in the industry is that the services offered by security service is _____, whereas the goods are _____.
3. Become knowledgeable about the customer's _____.
4. The security company should take "_____" to review its overall performance and approach to the market-place.
5. It is particularly important in the security industry to avoid a mission statement that reflects "product" rather than "_____."
6. Marketing is a critical function of the security organization. ☐ T ☐ F
7. Selling is the art of developing relationships. ☐ T ☐ F
8. An understanding of the customer's business is not important for the security supervisor in marketing security services. ☐ T ☐ F
9. The strategic plan defines the company's overall image. ☐ T ☐ F
10. The security supervisor has a responsibility to sell services personally. ☐ T ☐ F

This page intentionally left blank

6 Crime Prevention and Community Relations Strategies

Mark Gleckman and Christopher A. Hertig

The National Crime Prevention Institute defines crime prevention as the anticipation, recognition, and appraisal of a crime risk and the initiation of action to remove or reduce it.

Some definitions include the reduction of fear also. This is important as fear of crime may be a larger issue in some respects than the crime itself: "the perception is the reality" to some extent. Fear of crime also negatively impacts the quality of life.

Crime prevention may also be thought of as *crime risk management*. This may make more sense from an operational perspective as protection programs may avoid, reduce, spread, transfer, or accept risks. Each strategy has its place. Once risks have been identified and assessed in terms of probability and criticality, they can be managed in various ways.

Crime prevention or crime risk management is central to fulfilling basic human needs. Abraham Maslow's Hierarchy of Needs has safety needs second in the sequence right after the first, basic need for survival. Safety needs include protection and security. Humans need this; citizens, employees, students, guests, and patients expect and demand it. A basic premise of "security" is that it preserves the ability of persons within a protected environment to use that environment free from harm, fear, or disruption.

Crime prevention generally focuses on the reduction of criminal opportunity rather than working to inhibit the desire or the skill to commit the crime. Offender motivation is generally left untouched in physical security planning.

Potential victims can reduce criminal opportunity by understanding criminal attack methods and taking precautions against them. Convincing community members to take basic precautions is the main task of crime prevention. Communities may be residents in a neighborhood or building. Community may also be tenants in a shopping center, students in a school, or employees in a retail store. There are many types of communities; in some cases, crime prevention efforts will work with several different communities.

Crime prevention practitioners work to inform the community that criminal opportunity arises out of carelessness. Inadequate locking devices or poorly secured doors are all the criminal needs. Crime prevention practitioners want the community to be aware that criminal opportunity arises because of carelessness, inadequate or lack of elementary locking devices, and doors that any novice could get through.

Crime prevention specialists must possess a wide variety of general knowledge in crime prevention theory and practice. They must be adept at public speaking and promote good community–police relations at all times. Furthermore, they must have a thorough knowledge of the area, the people in it, their needs, and projects and programs that will aid the community in developing a comprehensive crime prevention program. Crime prevention specialists must be students of criminology, local crime trends, and crime interventions. That

is the "steak" of crime prevention. They must also be leaders and teachers. Effective crime prevention programs involve large doses of positive community relations. Community relations and marketing are the "sizzle" needed to sell the "steak."

One impediment to professional progress is the separation of the crime prevention community and the security industry. The crime prevention community and the security industry do not talk to each other as much as they should. Crime prevention personnel are most often allied with criminology, policing, and community outreach programs. Their professional identity does not lie with physical security as does that of the security industry. Crime prevention personnel in the United States are primarily, in fact almost exclusively, publicly employed. A significant number are volunteers. Security professionals are largely privately employed. This is unfortunate as both "camps" can learn from each other. It also does not support the movement to effect liaison between various sectors in the effort to provide for better Homeland Security. The challenges posed by terrorism, organized crime, and economic crime are transnational. They certainly deserve multidisciplinary study rather than a "siloed" approach.

Academics and practitioners would do well to investigate the research and resources of the other "camp" in order to obtain the best methodology. Professional organizations can take a leading role in this regard.

Crime Prevention and Response Theory

In earlier chapters of this text, Mary Lynn Garcia's model for the design of a Physical Protection System (PPS) was discussed. So too were criminological theories, a principle one being Routine Activity Theory. Mary Lynn Garcia has asserted that response to criminal attack is a key component of a PPS. Routine Activity Theory postulates that the absence of a capable guardian is a major factor in crime causation. Emergency management planning has *response* to emergencies as a key component. These perspectives are parallel to each other. And they raise issues in protection planning that must be addressed. If we solely focus on detection and deterrence but not response to crime problems, our management of them will be reduced to a piecemeal attempt. Unfortunately, in traditional crime prevention and physical security planning methodologies, the response aspect has not assumed a dominant role.

Furthermore, response is largely within the province of the protection officer and the investigator. They are the folks who must deal with the aftermath of criminal activity. As the mission of the International Foundation for Protection Officers is to educate, train, and certify security personnel, response to crime assumes a central role. The foundation has addressed this by initiating the Crime and Loss Investigation Program, a certificate course designed to develop more rounded knowledge of investigation, intelligence, and interviewing in participants. Postevent investigation can be considered as part of response to crimes and other loss events. American Society for Industrial Security (ASIS) International's research arm, the ASIS Foundation, has conducted a Victim Services Awareness Survey, the purpose of the survey being to aid in the creation of victim service materials and partnerships within the realm of private security (http://www.asisonline.org/foundation/victims.pdf, Accessed on March 8, 2007). Both organizations' initiatives illustrate an awareness of the response to crime.

As we begin to apply theoretical principles to crime risk management, response becomes very important. *There has to be a follow-through within protective planning*. In this chapter, we attempt to emphasize Response along with Detection, Deterrence, Denial, and Delay as appropriate.

Other considerations in crime prevention are as follows:

1. **Crime may be area-specific to a substantial degree.** Generic measures may not be adequate to deter criminals in all cases. The higher the motivation of the offender, the greater the obstacles necessary to deter.
2. **Layered defenses or "defense-in-depth" is an important concept that should be integrated into protection plans.** The "bundling" of protective measures in a system placing

increasingly difficult obstacles in the adversary's path is "defense-in-depth." Military organizations have employed this concept for hundreds, if not thousands, of years. IT security folks do this today, even though their terminology may be different.

3. **Deterrence occurs and is the basis for Beccaria's theories on general and specific deterrence as well as Rational Choice Theory.** Unfortunately deterrence is difficult to measure. A prudent approach is to bundle protective measures together and add new ones to increase the probability of deterrence. Each measure has some deterrent value but how much is often a guess. Layered defenses providing an accumulation of deterrence is the prudent course of action.
4. **Crime reduction measures have a life span of effectiveness.** Initially a crime reduction measure will make the crime rate drop. After a period of time the rate will increase. It does not, however, reach the level it had before the intervention was implemented. Crime is fluid and so protective measures must also be fluid. Periodic modification based on continuous assessment is a necessity. One must have metrics for determining the effectiveness of crime reduction measures.
5. **Protective measures are best employed when they address multiple issues.** Closed Circuit Television Equipment (CCTV) may detect and deter and provide an investigative aid for robbery attacks. It may also help manage other types of criminal activity, ranging from shoplifting to terrorism. Lighting may deter some criminals; it also enhances safety. Maintaining a standoff zone in a parking lot protects against vehicle-borne explosives; it may also impede access to dumpsters by employees who have secreted items there for later retrieval.
6. **Crime prevention/security research is usually lacking.** Advice is given without validation. One means of correcting this is to use international sources. Policing and crime prevention have a much richer history in the United Kingdom than in the United States. Studying what other countries have done provides a more holistic understanding of the crime risk phenomena.

Community Considerations

Each "community" that is being protected has different needs and characteristics. There are cultural, demographic, and budgetary factors that must be taken into account before any reasonable protection plans can be implemented. Knowing the "community" then is of paramount importance.

Whether called community watch, citizen alert, business watch, neighborhood watch, or block watch, the idea is the same—neighbors watching out for each other. The concept involves developing a crime prevention program in which citizens work with each other and with local protection agencies to reduce crime and vandalism in their community. One variation of this is "corporate crime watch" or "business watch." Such programs can be useful in detecting traveling criminal groups such as professional shoplifters or con artists. They may also help to spot terrorists conducting surveillance or in the location of lost persons (children or senior citizens).

Criminals gravitate to places where they feel safe and secure. They stay out of neighborhoods where they are likely to get caught. The goal of community watch programs is to make criminals aware that their activities are being watched and will be reported to the police. In neighborhoods where people watch after each other, burglary rates are lower.

Participation in a community watch program does not require a great deal of time. However, it does require you to become slightly more observant in your daily routine and maintain open lines of communication with your neighbors and with local law enforcement. If everyone participates, a community watch can work to reduce crime and make your neighborhood a safer place to live. Having signage indicating the presence of a community watch, "Block Watch," or other similar program bundles the deterrence measures together and increases their effectiveness.

Crime Free Multihousing is another variation of community crime prevention. It originated in Mesa, Arizona, and uses a neighborhood watch program within multihousing

properties. Crime Free Multihousing uses the resources of local police, property owners, and residents. It consists of three key elements:

1. Management training in how to deter illegal activity.
2. Security assessments (surveys).
3. Resident training and involvement (Harr, 2005).

In addition to community watch programs are contractual security arrangements. The new paradigm for protection involves private security forces working in concert with public police. This takes many varied forms from contract security agencies patrolling housing projects and gated communities to proprietary security forces protecting governmental property. There are also initiatives where contract security forces patrol downtown districts through arrangements with merchant's associations.

Assessment of crime control needs, combined with effective utilization of resources, is key to crime prevention programming. Thinking creatively can make this happen. Traditional thinking will stifle it.

The Security Survey

A security survey is an on-site physical examination of a home or business and its surroundings and environment. The security survey will evaluate the security of the property, identify any deficiencies or security risks, make recommendations to reduce or eliminate any threats and/or vulnerabilities, and determine the degree of protection needed. Surveys are normally conducted by security consultants or police department crime prevention officers. The former provides more in-depth analysis at a significant cost. The latter provides rudimentary information at no cost. Each, however, gives an external, objective analysis. Proprietary personnel can perform surveys but having an external review gives more credibility to the process.

Surveys are used to diagnose and prescribe protection programs and measures. That is their primary purpose. They also give the property manager a chance to assess how users view security and management. Surveys demonstrate concern by management and can help facilitate the development of greater security awareness: astute managers may have several people involved in this project with a consultant acting as coordinator. Security surveys also provide an opportunity to distribute crime prevention information.

The survey team or specialist should review any information that may be available from previous studies and recommendations. They should assess loss trends and facility user perspectives and explore both insurance and tax savings. Their research will consist of file review, interviews with managers, and questionnaires of facility users. They will also incorporate a checklist to facilitate the gathering of pertinent information. The checklist is considered to be the backbone of the survey and will serve to systematically guide the specialist through the areas that must be examined.

Checklists can take many forms. They can be a simple list of questions requiring only a yes or no response or they may ask open-ended questions requiring some narration. It does not matter how a checklist is designed as long as it provides a logical way to record information and ensures that no important questions go unasked. Checklists can be generic to begin with, but they should evolve into a customized list for each environment.

At the conclusion of the survey the specialist should prepare a report. The report should explain the most serious vulnerabilities and then provide a menu of options for addressing them. In this way the survey is both diagnostic and prescriptive, although it should be written in such a manner that the manager receiving it makes the decision on how to address the issues. The specialist should then discuss the results with the client and explain the recommendations.

Home Security—Burglary

Home security may not seem to be within the province of the protection professional who is concerned with securing business, nonprofit, or governmental environments. Home secu-

rity, however, is an area for which protection personnel may offer consultation. It is also part of estate security for VIPs as well as for managers' homes during times of elevated threat levels (strikes, domestic violence, terminations, animal rights or eco terror group activism, etc.).

Home burglaries in the United States generally occur during the day when the residents are not at home. Entry is about evenly split between the front door and a rear basement window. Some household burglaries occur without forced entry by opportunists who happen to spot an open window or door, an unlocked gate, an open garage, or a house that looks like the occupants have not been around for a while. Burglars generally target cash or easily disposable valuables. Note that these change over time and area. Stealing bicycles may be prevalent in one time/place while theft of scrap metal is dominant in another.

Burglars have a "prowl" or set method by which they move about inside a premises. Investigation looks at what was targeted as well as entry and exit points, the prowl, and postevent behavior such as escape from the scene and disposition of the stolen property. Burglary is "cleared" about 15% of the time: there are no witnesses and fingerprints are usually of little use due to the prints of the residents. Tool marks, significant modus operandi, neighborhood canvasses, and crime analysis are all techniques used to apprehend burglars. In many cases burglars operate in rings; once one burglar is apprehended he or she often confesses to a string of offenses.

Burglars are usually teenagers (amateurs) or young adults. There are varying levels of sophistication to burglary attacks. This progresses upward from finding unlocked doors to using brute force (kicking, shoving, or use of a sledgehammer). From there burglars may effect an unskilled attack with a large screwdriver, pry bar, or tire iron. Professional burglars use intel/reconnaissance/casing as well as special tools and skills. Pick guns, lock rakes, dent pullers or "slam hammers," etc. are used.

While burglary is the primary loss event in homes due to the malevolent acts of humans, it is not the only one. Robberies may also occur. Rapes are possible. So too are acts of voyeurism and exhibitionism. If burglary is the original loss problem, a *cascading effect* may happen where it develops into something else. Identity theft/fraud is certainly an eventuality.

The following PPS countermeasures offer some help in developing a home crime prevention plan. The list is not exclusive, rather illustrative. Protection professionals will develop their own lists after assessing the environment to be secured.

Deter

Trim hedges below window sills. Prune tree branches 6 ft up and away from your home.

Do not let newspapers or mail accumulate. Keep your lawn and shrubs cut.

Light up all exterior doorways and shadowed areas. Use PIR motion detectors or photoelectric sensors for exterior lighting. This provides both security and safety.

Use UL-rated automatic timers to turn on and off your lights, radio, and television. Set the radio or television to a talk show or news station.

Make sure that all exterior doors are solid core and that all exposed hinges are pinned or spot welded.

Use auxiliary locks on all windows and sliding glass doors.

To ensure windows cannot be lifted out of their track, install additional metal screws into the upper track.

Install an alarm system. Make sure that the alarm company sign is also posted. In this way protection measures are "bundled," a key ingredient to crime deterrence. Also have the alarm system zoned. Use a UL-listed central station provider.

Get a dog. Even a small dog may discourage a burglar. Dogs are mobile alarm systems. They do, however, require extensive care and incur expense over time (chewed up shoes and veterinary bills), so purchase of a dog is a serious personal commitment. Also be careful about owning "dangerous breeds" as some homeowners polices will not cover houses with large dogs (most large dogs are considered "dangerous breeds").

Deny

Avoid hiding keys outside. Burglars know where to find them.

Engrave valuables with your driver's license numbers to prevent resale ("fencing") of the items.

Delay

Secure sliding glass doors so that they cannot be lifted out of their tracks by using extra screws in the track. These are set higher than the original screws.

High-quality locks with at least a 1in. dead bolt are recommended. With the rise in "bumping" attacks it is prudent to use locks where the key blanks are controlled. Dead bolt locks on all doors also enable one to obtain a reduction in insurance premiums.

Consider auxiliary locks, especially double cylinder dead bolts on doors. This may provide some additional protection against "bumping" attacks.

Detect

Get to know one's neighbors and watch each other's homes.

Consider a home alarm system. This can be a local alarm or a central station arrangement. Explore all cost factors before installation. These include purchase, installation, maintenance, monitoring, insurance savings, insurance requirements, false alarm ordinances, etc.

Respond

Keep an inventory of valuables and their serial numbers. Photographs can also be used.

Engrave your valuables with your driver's license number so that they can be traced by law enforcement agencies.

Consider off-site storage of information on computers. Backup options for data should be explored in the event of theft of a computer.

Have a commercial central station alarm monitoring agreement with a UL-approved company. Video and audio recording systems may aid in apprehending the perpetrators. Within a secured perimeter a proprietary central station system may be used.

Utilize a proprietary security force as part of an estate protection plan or within a gated community.

Have house numbers that are at least 4 in. high, illuminated, and mounted on a contrasting background.

If you come home and find signs of forced entry, do not go in. Go to the nearest phone and call the police.

Home security does not have to cost a lot of money. It just takes a little extra time and some common sense. Eliminate the opportunity and the offender may not be as motivated to target the home.

Robbery

Violent crimes, such as robbery, can cost the business owner not only a financial loss but also a loss of life or serious injury. Robberies can turn into hostage situations or homicides. Robberies comprise the majority of workplace murders. Note that there are many types of robberies ranging from the "mugging" of an individual to "home invasions" to restaurant heists to armoured car "knockoffs."

Isolated stores like convenience stores and small minimarts at gas stations are especially vulnerable to robbery. Retail robbery targets include cash registers, cash rooms, and cash deposit runs. Convenience stores may be targeted by drug addicts whose reasoning process is seriously impaired. They may also be hit by "spree robbers" who commit numerous offenses within a small window of time.

A typical robber is male, between 20 and 29 years old, and armed with a handgun. He is likely to be nervous and may become violent if surprised by a sudden motion, an audio

alarm, or the arrival of police. The clearance rate for robbery averages about 25% in the United States. Robbers are aggressive criminals; they are not deterred as much by being seen and recognized as shoplifters or burglars. Robbers are "motivated offenders"! They will most likely be dissuaded by the prospect of a low "score" (an unsuitable target) and an impeded escape route.

Robbers sometimes follow a sort of "career ladder" (Figure 6.1). They may begin with unarmed "mugging" and progress from there. Generally the street robberies (muggings) are committed by offenders in their late teens. Convenience stores may be targeted by those same persons who are now in their early 20s and so on. Older, bolder, more organized robbers hit banks and armoured cars.

Robberies often involve the participation of an insider. A current or former employee is commonly seen with restaurant and armoured car robberies. The level of involvement may range from passive, where information is supplied, to active participation in the robbery itself. Whatever the particular scenario, it is important to remember that robbers look for what they consider to be suitable targets.

Robbery prevention will involve a combination of training and security hardware. An effective robbery prevention plan can be designed and implemented by determining local crime trends and the facility's high-risk areas. Robbery, like burglary, tends to be

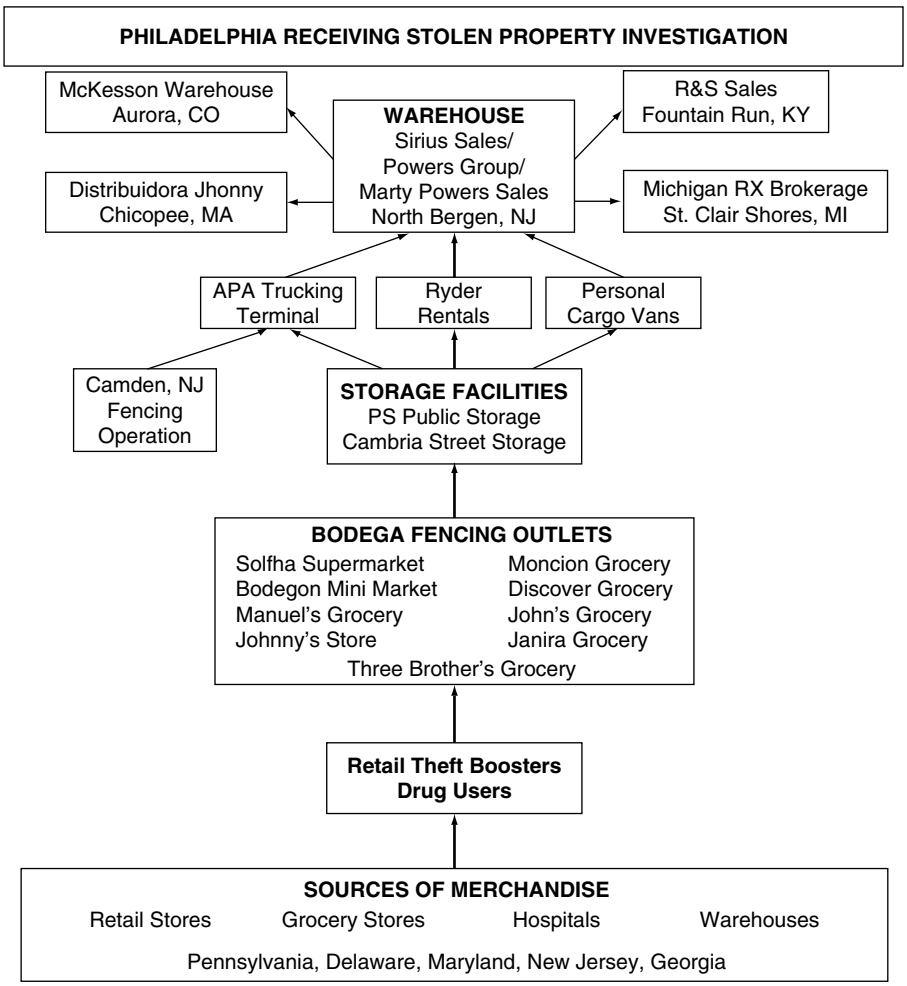


FIGURE 6.1 Robber career ladder.

area specific—although this may not be as true as it once was. Utilizing commercial crime risk services such as capindex.com can aid in better understanding of the robbery risk.

The most cost-effective robbery deterrents are to decrease the amount of cash on hand and increase the visibility of clerk areas. Having two clerks on duty during peak robbery hours (generally 2000-0400) may also be effective but at an added cost. Security hardware such as cash storage devices, metal detectors, or CCTV has proven to be effective in reducing robberies, but each measure needs to be researched thoroughly before being implemented. The following are some suggested robbery prevention and management methods following the concepts of deterrence, denial, delay, detection, and response. Note that specific measures may be relevant only to particular types of robbery events.

Deter

Walk with confidence and be observant of your surroundings. Make appropriate eye contact and do not walk into groups of people if at all possible.

When carrying a purse, keep it over the shoulder and clasped with one arm to the body.

If possible walk in groups.

Keep the amount of cash in the register to a minimum—under $100.00.

Never display cash in public view.

Post signs stating that employees cannot unlock the safe.

Reposition window signs or displays that may be blocking the view of the register area.

All entrances should be kept well lit.

When taking a cash deposit to the bank, be totally unpredictable. Constantly change routes, times, methods of cash concealment, and deposit personnel.

Advise employees not to wear expensive jewelry to work.

Deny

Any entrance door not being used should remain locked.

Keep safes and money boxes locked when not in use.

Use dye packs that explode and stain both the money and the robber.

Delay

Use a time-delay cash-drop safe.

Secure all separate offices in the rear of the store.

Detect

Establish effective liaison with local police and other merchants. Robbery teams and individuals tend to work at specific times and in specific areas. They also tend to select certain types of targets.

Being observant of people's hands and eyes is important. So too is their dress and gait. If they are dressed in such a manner that a weapon is being concealed or walking unnaturally due to secreting a weapon, this should be noted.

Use a CCTV that continuously records and is constantly being monitored, preferably on-site.

Become "tail conscious" of persons following in a vehicle. The tailing vehicle may not be in good repair as felons often acquire and discard "junker" cars.

Respond

Train employees in robbery reaction procedures. These should include the use of calming techniques as well as methods of observation. There should also be procedures in place for protecting customers and isolating the scene so that investigation may proceed.

When confronted with a weapon, slowing down one's rate of speech and movement tends to have a calming effect. So too does speaking in a lower tone of voice. Doing things "slower and lower" helps to calm a situation.

It should be noted that many of the same skills necessary for good customer service are virtually identical with those needed to calm a crisis. The crisis may be a robbery or simply an agitated customer. Management should invest in strategies to develop these skills; doing so makes good business sense and is the socially responsible thing to do.

Giving space/creating distance between someone with a weapon and the accosted party also tends to have a calming effect. The assailant feels that he or she is superior and not being challenged as his or her personal space is being respected. Note that violent persons have greater personal space zones than the rest of the population. Give them lots of space! Additionally, having more distance from the weapon reduces the danger somewhat. A knife-wielding adversary must step forward to use the knife; a firearm must be aimed at a greater distance, etc. Instructional programs should emphasize this.

Duress alarms may be employed. These should be portable and/or in several locations. There should also be drills and practice in their use. Being tied up is a possibility; while this is not desirable it may be unavoidable.

Caparatta (1998) maintains that stashing paint scrapers at areas where they may be easily obtained can aid in cutting loose if victims are tied up. Offering to be tied up by placing your hands in front with the dominant hand (wrist) on top makes escaping easier. Use of "bait" money (numbered bills) may assist in the apprehension of a robber.

Use audio and video recording to aid in investigation.

Establish liaison with local law enforcement for dealing with robbery and potential hostage situations.

Consider having security department staff join in local police organizations, investigative organizations, and task forces.

Consider donations of funds, vehicles, and equipment to local police to aid them in investigation. The insurance industry in the United States has done this for many years.

Check security equipment daily and fix anything that is not working. Have an overlapping audit system in place for all cameras, alarms, and communications devices. This can consist of having users do a rudimentary check as soon as they assume their post/duty. There can also be supervisory checks on a periodic basis as well as performance testing by technicians on a preset basis.

After closing, never reopen for anyone. Opening and closing procedures should be taken very seriously. Ideally, a lone employee should not be doing this. There must also be an assessment of the area to discover persons who may be conducting surveillance.

Rape

Rape is a horrific crime that often has long-term serious consequences for the victim. For this reason alone, rape prevention and response should be addressed in crime prevention programs. The reporting rate of rape is lower than that of other crimes. It is embarrassing to the victim and she may not feel supported by those close to her about coming forth about it. Rape victims are generally young, unmarried women but they may be of any age or gender.

Deter

Avoid situations where a rapist could easily surprise, stun, and control you. Be careful when approaching your car: scan in all areas to see if anyone is around.

Maintain confidentiality. Allowing a potential rapist to know you are a lone female provides him with an opportunity, or at least the beginning of one.

Protecting one's privacy extends to the Internet. Unfortunately, there are many people who provide information about themselves without thinking. The Internet is, to a large degree, a haven for creeps. Once information is on it, there is no telling who can access it.

Avoid becoming intoxicated. At the same time be alert for any attempts to place psychoactive substances in your drink by anyone else.

Detect

As a significant portion of rapes involve dates or acquaintances, who may or may not be dates, a method of preventing rapes in these settings has been devised. The ACT Method of Date Rape Prevention is a simple acronym that outlines a prevention plan.

Assess

Assess the person being dated. Is he intoxicated? Does he have a negative view of women? Has he managed his personal affairs well or are there "unfinished sentences," sporadic relationships, or other indications of character flaws in his background. One example of an "unfinished sentence" was the serial murderer Ted Bundy. He was bright and articulate, luring women to their deaths. He had completed one year of law school—an "unfinished sentence." Migratory job history is another indicator of personal problems. So too is financial mismanagement.

"Control freaks" are better left alone also. While they may be difficult to spot in the opening phase of a relationship, any indicator of the prospective date being a "control freak" should be taken seriously. Such persons are used to having their own way and may not take "no" for an answer. Additionally, the annals of domestic violence are filled with abusive husbands and boyfriends who were overly controlling.

Persons with these characteristics should be avoided. So too should anyone you have a "funny feeling" about. Generally one's instincts are correct in these matters. Trust your instincts!

Control

Control the situation. Be sober. Have your own keys, own cell phone, and own car. Make some of the key decisions like deciding where to go and what to do.

Tell

Tell the date your limits. Be polite and considerate, but firm. Communicate verbally and through touch as appropriate in the situation.

Respond

Responding to rape attempts can include physically fighting back or psychologically distracting the adversary. Each approach has its merits; neither is appropriate in all situations. While rape is a physical assault, it often occurs in a social setting. This coupled with a hesitancy to become physically aggressive makes fighting back a limited option.

Noncombative options include vomiting, urinating, or defecating.

Verbal techniques may include discussing the rapist's mother or sister: "How would you feel if someone did this to your mother?"

If using physical force: fight fast, hard, and repeatedly. Not "hit and run," rather hit, elbow, kick, stomp, and then run!

And yelling all the while!!!!!!

Yelling serves as a distraction to the assailant. It also alerts bystanders and aids in breathing, which, in turn, helps with physical exertion. Yelling is good!

Responding also includes reporting the rape and following through with the legal system. The quicker the rape is reported the greater the chance of apprehending the rapist.

Additionally, rape victims should not wash, douche, or disturb anything at the crime scene.

Rape victims, like other victims, have physical, emotional, psychological, financial, and transportation needs. Crime prevention programmers should bear this in mind. Facilitating victims' needs is important for humanistic, legal, and community relations purposes. Astute protection professionals will seize upon every opportunity to aid victims. Note that much of this may be via referral to other organizations. Liaison with these entities is important. Know which organization provides which service.

Victims of rape, or other crimes, will have to deal effectively with the judicial system. The "3 'Ps' of judicial system management" are *patience, politeness,* and *persistence. Patience*

is required as things take time. *Politeness* is necessary as the key players in the justice system need to be the advocate for the victim. They cannot get agitated with them. *Persistence* is necessary as the case is one of many. Police, prosecutors, investigators, and judges are busy people. They may not take action on everything that is brought in front of them—at least not as fast as the victim may expect. Some diplomatic reminders along the way may be both appropriate and necessary.

Criminal defense attorneys generally use one of two defenses for rapists: mistaken identity or asserting that the act was consensual. When pressing a rape complaint, this should be borne in mind from the outset.

Consideration should also be given to pressing the issue in the civil justice system. Such an approach has numerous advantages. The outcome of the O. J. Simpson case where he was acquitted in criminal court of murder but convicted in civil court of unlawful death is a good example of this.

Rape victims should always remember that it is not their fault. It is the rapists' fault. Period. They should also be aware of their feelings and discuss the incident with a professional counsellor. Rape is a traumatic event, the total consequences of which may not be seen initially.

Identity Theft

The various forms of identity theft/fraud pose a significant problem to individuals, employers, and creditors. The cost of loss is very high: 700 hours to clean up bad credit. Additionally, as we develop new means of exchanging information, there will be a corresponding increase in the type and number of frauds perpetrated. Technology increases risk exposure while society expects more protection. Employers and businesses are increasingly being held to higher standards of care in regard to the protection of employee or student information. So too are health care and campus organizations. Principally, this is taking the form of legislation on both the state and federal level where organizations are required to alert customers, patients, or students if there has been a loss or compromise of their data. There are also industry standards such as those set by the Payment Card Industry, an association of major credit card companies (http://securitysolutions.com/news/restaurant-credit-card-security/, Accessed March 7, 2007). Industry standards are likely to expand. This, in turn, creates greater standards of care. Civil redress for information safeguarding and accountability lapses is the natural outgrowth.

Deter

Use a locked mailbox either at home or use a secure public mail collection point.

Deny

Shred all papers with your name, address, and account numbers on them. Do not shred envelopes that may have become contaminated with a biological agent.

Destroy all old, unsolicited, or unused credit cards.

Carry only essential credit cards and identification in your wallet. Eliminate unnecessary credit cards. Reduce the risk.

Keep a close watch on and control over wallets and purses. "If you can't afford to lose it—you can't afford to risk it."

Beware of "shoulder surfing" where someone observes a card number by watching over one's shoulder. This has variations such as in airport phone banks and with ATMs. Sometimes visual aids are used.

Only have your name—with first initial—on your personal checks.

Beware of Internet banks that are illegitimate. Check with the FDIC or Federal Reserve before making any deposits.

Never give out your account number or SSAN over the phone or Internet unless you are initiating the contact. Be certain that it is a legitimate organization that you are giving it to.

Consider unlisted phone numbers, being on "Do not call" lists.

Detect

Assess your public profile by "Googling" yourself. You should try several search engines to get a more complete and thorough picture.

Utilize an identity protection service that checks all three of the major credit bureaus. Identityguard.com, Equifax.com, creditexpert.com

Observe cashiers' and waiters' actions with your card. Some have been known to use a scanning device to capture the number.

Respond

Photocopy important documents and store "off-site" in a safe deposit box or relatives' house. This includes credit card numbers, driver's license numbers, etc. In the event of a loss, having these records helps to facilitate relations with creditors, motor vehicle bureaus, etc.

If victimized, keep a running log of the investigation. Get to know the investigators by name. Get their points of contact. Understand the areas of responsibility of each. Note times and dates of each contact with them.

Employers can play a key role here by setting up preplanned response systems and training employees.

Shoplifting

Shoplifters come in all sizes, ages, and sexes. They come from varying ethnic, educational, and economic backgrounds. In very general terms, shoplifters fall into two categories, the amateur and the professional. The amateur steals occasionally without a significant amount of preplanning. The professional steals for a living. The professional preplans, steals almost daily, and often steals in an organized group. Note that professionals are sometimes violent and assault loss prevention agents when they attempt to detain them. It is not uncommon for professional shoplifters to have associates waiting in a care outside to beat up, stab, or shoot any LP agents who interfere with their thefts or escapes. While there have been professional "boosters" around for decades, the emergence of Organized Retail Crime is a major concern. These groups are large, sophisticated, and connected with a variety of criminal activity. In some cases, professional shoplifting rings have funded terrorist groups. Shoplifting is not a small problem: the economic impact on the retailer is enormous and the connection with additional criminal activity extensive.

Consider a theft and fencing operation that took place in the Philadelphia area in 2005. When the ring was taken down, there were 48 arrest warrants and 64 search warrants executed. In addition to the Loss Prevention departments of various retailers, the following public agencies were involved:

- PA State Police
- Philadelphia Police
- INS Agents
- PA Department of Revenue Cigarette Tax Investigators
- NJ State Police
- The following protective measures aid in managing the shoplifting problem. They also target related criminal activity. Grabbing money from a cash register may not fit the statutory definition of shoplifting, but it is a loss event nonetheless.

Deter

Maximize visibility by raising the cash register area, using convex mirrors, one-way mirrors, and lighting.

Post signs in plain view stating that all shoplifters will be prosecuted.

Have domes or camera lenses visible.

Utilize uniformed personnel or extra sales staff. This can be adjusted based on sales volume and historic crime trends for the area the store is in.

Deny

Have the cashier staple the customer's bag closed with the sales receipt attached.

Use an electronic article surveillance system (EAS).

Keep cash registers locked and monitored at all times.

Delay

Use EAS tagging, which must be removed.

Design controlled egress paths so that quick exits are diminished to a degree (difficult to balance with marketing and evacuation considerations). This may help in discouraging "smash and grab" attacks.

Detect

Sales associates should greet and make eye contact with customers. This is good customer service combined with deterrence.

Cashiers should verify every item's price if there is any question regarding it. When cashiers guess at a price they generally underestimate it. Verifying prices also may detect attempts at price switching.

Cashiers should check every item sold that might hide other merchandize. Seeing the bottom of the cart is essential.

Liaison with other merchants, mall security, and police forces should be established so that active shoplifters are identified as soon as they arrive on-site.

Respond

Camera systems with digital recording capabilities.

Develop policy and procedures on apprehension, interrogation, civil demand, etc.

Establish liaison with police prosecutors and judiciary regarding prosecution.

Conclusion

An effective crime prevention program is so extensive that it will demand a concerted and coordinated community effort. Citizens, students, and employees must be educated to recognize certain conditions and situations that contribute to crime. These community members must be motivated to report and eliminate crime causing conditions. They must identify and report potential criminal behavior. Individuals must come to realize the need to protect themselves against crime and to safeguard their communities (neighborhoods, workplaces, schools, etc.)

Contemporary crime is multifaceted. What may appear as a simple shoplifting may in fact be a "fund-raising" operation for a terrorist organization; burglaries become identity theft/frauds. Organized criminal activity in its varied forms will continue to be a major challenge to the citizenry of a free society. Economic crime, whether perpetrated by organized groups or individuals, threatens the finances of individuals, organizations, and even nations. Add to these public protection resources that are stretched very thinly. Crime prevention must be carefully planned and implemented using existing resources wisely. Everyone has a part to play.

References

P. Caparatta (1998). *Merchants at War: Survival Tactics for Armed and Unarmed Merchants*. Kansas City, KS: Varro Press.

L. Fennelly (2005). *Spotlight on Security for Real Estate Managers*. Chicago, IL: Institute of Real Estate Management.

J. S. Harr (2005). The Property Manager as Juggler."In *Spotlight on Security for Real Estate Mangers*, ed. L. Fennelly, Chicago, IL: Institute of Real Estate Management.

N. Jones (2006). "Organized Retail Theft." Presentation to the Central Pennsylvania Chapter of ASIS International, Harrisburg, PA, on June 15, 2006.

National Crime Prevention Institute (2001). *Understanding Crime Prevention*. Woburn, MA: Butterworth-Heinemann.
R. L. O'Block, J. F. Donnermeyer, and S. E. Doeren (1991). *Security and Crime Prevention*. Newton, MA: Butterworth-Heinemann.
K. C. Poulin, andC. P. Nemeth (2005). *Private Security and Public Safety: A Community Based Approach*. Upper Saddle River, NJ: Pearson Prentice Hall.

Crime Prevention and Community Relations Strategies

Quiz

1. The National Crime Prevention Institute defines crime prevention as the anticipation, _____ and appraisal of crime risk.
2. Protective measures are best employed when they address _____ issues.
3. A qualified crime _____ specialist should be used to conduct a security survey.
4. Yelling at an assailant while fighting back _____ him, _____ others nearby and aids in _____ so that physical activity can be performed better.
5. Deter, _____, Delay, _____, and _____.
6. The crime prevention specialist should limit their knowledge only to preventive measures. ☐ T ☐ F
7. A security survey is an on-site physical examination of the property which is both diagnostic and prescriptive. ☐ T ☐ F
8. Robbers are usually deterred by being seen. ☐ T ☐ F
9. Response to criminal attack is a key, if traditionally overlooked, aspect of crime prevention and physical security planning. ☐ T ☐ F
10. The "3 Ps" are: _____, _____, and _____ when filing a criminal complaint.

7 Public–Private Sector Liaison Programs

Brion P. Gilbride

The Liaison Function

As with other criminal justice disciplines, it has become more common in the past several years for private security agencies to become involved in partnerships with other agencies, government entities, and some nonprofit organizations. These relationships are often based on an exchange of information or intelligence, and in some cases involve sharing resources, training materials, or policy advice.

In their report on the subject, authors Gunter and Kidwell use Webster's definition of *liaison*, which is "communication for establishing and maintaining mutual understanding and cooperation (as between parts of an armed force)."[1] It was established in a report authored by Greenburg and Morabito on private–public sector relationships that while there are approximately 677,000 law enforcement officers in the United States, there are currently more than 2,000,000 private security personnel.[2] In addition to these numbers, the report also notes that the 9/11 Commission estimated in its report that 85% of US infrastructure is privately owned.[3]

These numbers mean that although the public sector agencies are charged with investigating and prosecuting criminal and/or terrorist activity, many of the physical locations involved will be controlled by the private sector. Many of the personnel involved in securing the crime scene, conducting initial interviews and interrogations, securing possible suspects, preserving evidence, and protecting a strategic location from harm, are likely to be private sector personnel such as security officers, armed guards, or perhaps the technicians who maintain CCTV, access control, environmental control, and other systems. The importance of all this can be summed up in this quote from Greenburg and Morabito:

> *Local law enforcement and private security organizations working together is vitally important to homeland security; the private sector owns or protects the overwhelming majority of the country's infrastructure, but local law enforcement tends to possess any threat information regarding that infrastructure.*[4]

---

[1] W. Gunter, and J. Kidwell. Law Enforcement & Private Security Liaison: Partnerships for Cooperation. Miami, FL: International Foundation of Protection Officers. Available: http://www.ifpo.org/articlebank/lawprivateliaison.html

[2] S. Greenburg, and A. Morabito. *Engaging the Private Sector to Promote Homeland Security: Law Enforcement-Private Security Partnerships*. Washington, DC: U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, September 2005, pg. viii.

[3] Greenburg & Morabito, pg. 1.

[4] Greenburg & Morabito, pg. 1.

Partnerships between private and public law enforcement are not new. The head of the first major private security agency in the United States participated in such activities. That man was Allan Pinkerton, founder of the Pinkerton Detective Agency. Pinkerton established his detective agency in 1850 after careers as a county sheriff and a detective for the city of Chicago. In 1861, while investigating an unrelated case, Pinkerton uncovered a plot to assassinate President Abraham Lincoln and warned him. Lincoln then hired Pinkerton to establish a "secret service," which was used to gather intelligence on the Confederate military; Pinkerton himself participated under the alias of "Maj. E. J. Allen."[5] After the war ended, Pinkterton returned to his Detective Agency, and the "secret service" he founded eventually became the US Secret Service, charged with protecting the President, among other duties.

Successful US Programs

There are notable examples in the United States of successful liaison programs between the public and private sectors. The New York City Police Department (NYPD), which is consistently the leader in pioneering new policing techniques, has a liaison program, as does El Paso, TX. Target Stores has its own program as well. The US Department of Justice has also issued reports on the liaison function. The following is a synopsis of these programs and reports.

NYPD Shield

The NYPD established its program, initially called the "Area Police/Private Security Liaison," or APPL, in 1986. It began with 30 and currently has more than 1,000 organizations participating. As part of the program, police officials review and evaluate security and evacuation plans for its member organizations' facilities. A communications network has also been established so that the APPL and member organizations can send and receive alerts and bulletins.[6] This program has now been placed under the umbrella called "NYPD SHIELD."

The NYPD Web site describes NYPD SHIELD as "a central destination for private sector security managers to obtain information and engage police department resources."[7] The program provides intelligence and threat information to private sector managers, and does this via formal briefings, electronic mail/bulletin board messages, as well as through informal conferences with local counterterrorism officers. The program is intended to furnish information to help private sector security officials counter the threat, and in return ask those same officials to help NYPD when the threat concerns private-sector properties. According to a brochure made by the NYPD, the security managers can request that counterterrorism teams be deployed, request intelligence and threat information, training for security personnel, assistance in physical security planning, and critical incident response. For more information, see the program's Web site: http://www.nypdshield.org

LEAPS El Paso

The "Law Enforcement and Private Security" organization, or LEAPS, was established in El Paso, TX, to foster a cooperative environment between law enforcement and the various private security entities operating in that city. The Internet Web site for LEAPS describes its mission as:

> *…to promote the concept of crime prevention; to enhance communication; and to encourage joint cooperation between law enforcement agencies, corporate security,*

---

[5] Author Unknown. Detective Allan Pinkerton Was Born in Glasgow, Scotland. Washington, DC: Library of Congress, Available: http://www.americaslibrary.gov/cgi-bin/page.cgi/jb/nation/pinkerto_2

[6] Greenburg & Morabito, pg. 11.

[7] Author Unknown. *NYPD Shield*. New York, NY: New York City Police Department, Available: http://www.nypd2.org/nyclink/nypd/html/ctb/shield.html

and private security organizations to reduce the opportunity of crime within the City and County of El Paso, Texas.[8]

LEAPS El Paso grants membership to those actively working in law enforcement or private security, and those persons must be of good character. Organizations and companies may also join, provided they designate a representative to act on their behalf. The representative must also meet the membership criteria.[9] LEAPS also endorses the "Advanced Security Training Course", a 40-hour course offered at El Paso Community College, for training purposes.[10] For more information, see the program's Web site: http://www.leapselpaso.com

Target & Blue

Not only are liaison programs promoted in the public relations sphere by law enforcement agencies themselves, but also by the private sector companies that enter into them. Target Stores, which runs a chain of department stores throughout the United States, started a program called "Target & Blue". According to a Target press release, the program "…shares technology, expertise and resources through local law enforcement partnerships and grant donations."[11] "Target & Blue" funds initiatives such as "Safe City", which has been successful in Minneapolis, MN. What "Safe City" does is establish zones wherein police resources are enhanced via partnership with Target Loss Prevention and donations for equipment from Target Stores. The Safe City program resulted in a reduction in crimes such as burglary, auto theft, and robbery since it became active in Minneapolis. This program will soon be expanded by Target Stores also in Tucson, Houston, Dallas, Philadelphia, and Cincinnati.[12]

Successful International Programs

In addition to programs in the United States, there are also successful programs in other countries wherein private security and government interface in a similar fashion. One such program is in Karachi, Pakistan and is called the Citizen-Police Liaison Committee (CPLC). In a research summary by Mohammad O. Masud drafted for the Centre for the Future State in 2002, Masud indicates that the program began in 1989 as a private organization in Karachi run by local businesses after a spate of kidnappings and other high-profile crime that affected the Karachi economy, which supplied the bulk of federal revenue for Pakistan. The CPLC is modeled after the British "neighbourhood watch" programs. The committees were established at four locations in Karachi and began their work by creating a database of stolen automobiles. The committee's work was extended to analyzing crime data for all of Karachi. The committee further provides citizen access to police services and operates informally so as not to unduly influence government operations as the police in Pakistan are considered by the public to be corrupt.[13]

Operation Cooperation

"Operation Cooperation" is a program begun by the Bureau of Justice Assistance, which is under the Office of Justice Programs in the U.S. Department of Justice. It was initiated to

---

[8] Author Unknown, Available: http://www.leapselpaso.org

[9] Author Unknown, Available: http://www.leapselpaso.org/join.htm

[10] Author Unknown, Available: http://www.leapselpaso.com/resources.php

[11] Target Corporation. *Target & Blue and Safe City*. (California, 2007) Available: http://pressroom.target.com/pr/news/community/other-community/PRN-safe-city.aspx

[12] Target Corporation. *Target & Blue and Safe City*.

[13] M. O. Masud, "Research Summary #17 – Co-Producing Citizen Security: the Citizen-Police Liaison Committee in Karachi" (Centre for the Future State, UK, 2002). Available: http://www.ids.ac.uk/gdr/cfs/index.html

determine the degree of cooperation between private security and public law enforcement, what types of cooperation were occurring, and how best to facilitate further cooperation between the two camps. The report on "Operation Cooperation" lists the following benefits of cooperation: networking, collaboration on specific projects, increased crime prevention & public safety, cross-fertilization, information sharing, and leveraging of resources.[14] "Operation Cooperation" identified activities common among liaison groups, such as:

- Networking—lectures, speeches, directories, and awards;
- Information sharing—crime trends, employee criminal activity, group e-mail lists, etc.;
- Crime prevention—use of CPTED and community policing, joint efforts on video piracy, graffiti, false alarms, and National Night Out;
- Resource sharing—expertise, funds, vehicles, facilities, and equipment;
- Training—evidence handling, alarm systems, and management;
- Legislation—drafting laws and ordinances for officer licensing, alarms, and specific criminal activity; and
- Operations—incident planning, joint operations, financial or computer fraud investigations[15]

The report on "Operation Cooperation" can be found in a variety of places, to include the International Association of Chiefs of Police at the following Web site: http://www.iacp.org

IACP/COPS 2004 Recommendations

In 2004, the Community Oriented Policing Services (COPS) office of the U.S. Department of Justice in conjunction with the International Association of Chiefs of Police issued a set of policy recommendations for the liaison relationship between private security and law enforcement. Collaborating on this were the American Society for Industrial Security (ASIS), the International Security Management Association (ISMA), the National Association of Security Companies (NASCO) and the Security Industry Association (SIA).

In addition to exploring the positive benefits of liaison relationships, the report also addressed negative aspects. For example, the report listed the following reasons the liaison relationship might fail:

1. Departure of the facilitator(s),
2. Egos & turf battles,
3. Lack of resources or a recognizable product,
4. Overemphasis on structure and resources,
5. Insufficient commitment from management,
6. Overemphasis on social aspect of meetings, and
7. Unwillingness to openly share information (perception of the sharer).[16]

The report also encouraged the government to get more involved in promoting law enforcement/private security liaison relationships. It encouraged the Department of Homeland Security (DHS) and the Department of Justice (DOJ) to contribute a variety of resources:

1. Increase research into this field
2. Study foreign countries' relationships between police and security

---

[14] International Association of Chiefs of Police & U.S. Dept. of Justice, Bureau of Justice Assistance. *Operation Cooperation*. Washington, DC: Office of Justice Programs, U.S. Department of Justice, 2000, Available: http://www.iacp.org, pg. 2–3.

[15] "Operation Cooperation", pg. 6.

[16] U.S. Dept. of Justice & International Association of Chiefs of Police. *National Policy Summit: Building Private Security/Public Policing Partnerships*.... Washington, DC: IACP, 2004. Available: http://www.iacp.org, pg. 17–18.

3. Produce an annual report on the size/scope of private security operations
4. Determine "best practices" for public and private officials to deal with terrorism, disasters, and other mass casualty incidents
5. Increase training opportunities
6. Establish a joint command college to train law enforcement and private security executives
7. Use existing programs for cross-training such as Federal Law Enforcement Training Center (FLETC) programs, ASIS programs such as Certified Protection Professional (CPP)
8. Encourage law enforcement to cover liaison activities in academy training
9. Create advisory council to oversee implementation of these ideas[17]

These reports came out in 2000 and 2004, and the recommendations made are promising. The "Operation Cooperation" report gives a variety of examples of liaison relationships in the United States, but as things stand in 2006, it does not appear that much progress has been made in furthering the liaison relationship. This is one context out of many that the Security Manager can create a positive image of both the department and its leader.

Selecting a Liaison

The most important aspect of establishing a public–private sector relationship is to select the appropriate person(s) for the job. This might include running the liaison program, attending meetings, drafting memoranda or even legislation, arranging trainings, etc. Therefore, this would not be some sort of "collateral duty" that can be thrust upon anyone available. Nor does it mean that someone could perform this function in one's spare time. There is no substitute for someone who believes in and is passionate about one's work with the liaison program, and this is true regardless of whether that person is on the private- or public-sector side. In essence, there has to be one committed person from each sector willing to work to make this happen—one has to be able to "sell" the liaison relationship to one's own superiors.

The police-security liaison began to make more sense to both sides after the 9/11 attacks, however in the five years not as much progress has been made in this arena as is clearly possible, given the ways in which law enforcement and private security can complement one another. A security manager that can find a public-sector partner with whom to make the liaison program work will increase the bottom line for his employer or contractor by (1) having greater access to police resources to resolve issues, and (2) create public relations value for the law enforcement agency and the employer by promoting the partnership.

Public–Private Sector Liaison Programs

Quiz

1. How much infrastructure in the United States is privately owned?
   a. 20%
   b. 45%
   c. 65%
   d. 85%

2. How many private security personnel are there in the United States, approximately?
   a. 2 million
   b. 1 million
   c. 500,000
   d. 100,000

[17] "National Policy Summit: Building Private Security/Public Policing Partnerships…" pg. 19–22.

3. The liaison program operated by the NYPD is called _____.
4. Law enforcement has little information on threats to infrastructure.
   a. True
   b. False
5. NYPD's program was established in:
   a. 1976
   b. 1986
   c. 1996
   d. 2006
6. To be successful, the liaison needs to be:
   a. Focused
   b. A, c, and d
   c. Driven
   d. Passionate
7. The liaison committee in Karachi was formed due to an increase in:
   a. Arson
   b. Bombings
   c. Kidnappings
   d. Sex crimes
8. _____ was hired by President Lincoln to establish what later became the US Secret Service.
9. Target Stores' liaison program helps law enforcement by:
   a. Donating resources and services
   b. Supplying loss prevention officers to be deputized
   c. Prosecuting shoplifters civilly instead of criminally
10. Liaison groups, in addition to sharing information and resources, also become involved in training.
    a. True
    b. False

UNIT X

Legal Aspects

This page intentionally left blank

1 Legal Aspects of Security

Christopher A. Hertig

Introduction

Protection professionals work within a complex array of legal standards. Their daily functioning requires them to be knowledgeable of laws governing the employment relationships present in the workplace, civil and criminal laws, standards of practice, as well as a myriad of government regulations. Added to this mixture is the burgeoning repertoire of professional standards enacted by such entities as ASIS International, the Joint Commission on the Accreditation of Healthcare Organizations, the National Fire Protection Association (NFPA), and others.

Unfortunately, traditional texts on legal aspects have often focused on criminal law and civil liability. Scant coverage of administrative or regulatory law has been given. Almost no attention has been paid to the vast and complex spectrum of employment law. This chapter will provide a brief introduction of various legal aspects of which protection supervisors must be knowledgeable. It is an introduction from which the reader is encouraged to expand. It is for educational purposes and is not to take the place of competent legal counsel.

Key Terms and Concepts

Action—a formal legal proceeding by one party against another. *Cause of action* is the right that one party has to institute a legal proceeding. *Actionable* means furnishing legal grounds for an action.

Agent—an individual authorized to act for or in place of another (principal) who represents that person.

Americans with Disabilities Act (ADA)—a law signed by George Bush on July 6, 1990, that was designed to ensure equal opportunities to employment based on merit.

Title I covers employers of 15 or more employees, state and local governments, employment agencies, and labor unions and is under the jurisdiction of the Equal Employment Opportunity Commission.

Title II provides for nondiscrimination on the basis of disability in state and local governments. It covers public entities such as state and local governments and public transportation. It is enforced by the Department of Justice.

Title III provides for nondiscrimination on the basis of disability in public accommodations and commercial facilities, such as hotels, office buildings, and retail stores. Places of worship and private clubs are not covered by Title III. It is under the jurisdiction of the Department of Justice.

Arbitrary and capricious—willful and unreasonable action taken without regards to the facts or the law. Arbitrary and capricious is the standard by which courts will overturn the rulings made by an administrative agency such as the Occupational Safety & Health Administration (OSHA) or Federal Communications Commission.

Bloodborne Pathogens Act—OSHA's Occupational Exposure to Bloodborne Pathogens; Final Rule, Standard 29CFR, part 1910.1030 became effective on March 6,

1992. Known as the "Bloodborne Pathogens Act," this standard requires employers having one or more employees with occupational exposure to bloodborne pathogens to have an exposure control plan, adopt universal precautions to prevent the spread of bloodborne pathogens such as AIDS and hepatitis B, educational training programs, and medical record keeping.

Burden of proof—the obligation of establishing a requisite degree of belief in the trier of fact in a legal proceeding. The degree of proof is necessary to prevail. The burden of proof varies between different legal processes.

Reasonable suspicion—the degree of facts and circumstances necessary to make a prudent and cautious person believe that the criminal activity is afoot. Reasonable suspicion more than a mere suspicion for it must be based on articulable facts and circumstances. Police officers in the United States may conduct a search for weapons of the outer clothing (pat down) of persons whom they have a reasonable suspicion of committing, having committed, or be about to commit a criminal offense. Similarly, school officials under *New Jersey v. TLO* can search students for contraband if they have reasonable suspicion.

Probable cause—also known as "reasonable cause"; enough evidence for a belief in the alleged facts. An apparent state of facts is found after a reasonable inquiry. Circumstances are sufficient in themselves to warrant a reasonable man believing the accused to be guilty. The necessary evidence is used for arrest, search, or the issuance of an arrest or search warrant. Probable cause is also necessary to defend against suits for false arrest.

Prima facie—at first sight; evidence sufficient on its face to establish proof. The amount of evidence necessary to support a fact at issue without rebuttal by the opposing party. Prima facie is used at preliminary hearings to bind a case over to trial in criminal cases. It is enough to send a case to trial but is not enough to convict.

Preponderance of evidence—the majority or greater weight of the evidence. More probable than not. Preponderance of the evidence is the standard used in civil cases.

Clear and convincing proof—the amount of proof that results in reasonable certainty of the fact at issue. More than a preponderance of evidence but less than beyond a reasonable doubt. It is often used in labor arbitrations.

Beyond a reasonable doubt—fully satisfied; entirely convinced to a moral certainty. Reasonable doubt is the degree of doubt that would cause a prudent person to hesitate in acting on matters of great import to them. This is the standard of proof necessary in criminal cases.

Certiori—a writ issued by a superior court (appellate court, Supreme Court) to an inferior court (court of first instance, lower court, trial court) requiring that the inferior court produces records of a particular case. Certiori is used to inspect the lower court's actions in order to uncover irregularities.

"Color of law"—the misuse of lawful authority by a government agent. The power vested in the official is exercised unlawfully and is only done so due to the appearance of lawful authority. Actions are taken under pretense of law and clothed in state authority that violate the rights of citizens. Unlawful acts must be done by an official while that person is exercising lawful authority; the acts could not have occurred, but for the authority that the official possessed. Under 42 USCA, Section 1983, private persons can be found to be acting "under color of law" when there is significant state involvement in the activity. Such persons can be found civilly liable—as well as criminally liable—under federal law for civil right violations.

Contract—an agreement containing a promise or set of promises, the breach of which is actionable. Contracts can be either expressed (manifested in written or spoken words) or implied (shown by actions rather than words). Contracts consist of several key parts:

1. An agreement to do or not do a certain thing.
2. Between legally competent parties (consulting adults).
3. Based on genuine consent of the parties.
4. Supported by consideration (profit or benefit accruing to each party).

5. Made for a lawful objective, not in violation of public policy.
6. In the form required by law.

Equal Employment Opportunity Commission (EEOC)—an administrative agency created by Title VII of the Civil Rights Act of 1964. The Commission works to end discrimination based on race, color, religion, sex, age, or national origin in employment. The EEOC promotes voluntary programs of equal opportunity and also seeks to resolve disputes. The Commission may also assist in bringing actions based on a violation of Title VII on behalf of the aggrieved parties in the federal courts. The EEOC also enforces the Age Discrimination in Employment Act of 1967, Equal Pay Act of 1963, and those sections of the ADA that deal with employment.

Evidence—proof of a fact at issue. Any testimony, writings, exhibits, physical objects, etc. that may help prove the existence or nonexistence of a fact.

Negligence:

Simple negligence is failing to exercise the degree of care that would be exercised by ordinarily prudent persons.

Gross negligence is the intentional failure to perform a duty in reckless disregard of the consequences of nonperformance. Gross negligence is a conscious and voluntary act or omission likely to cause serious injury to another and of which the "tortfeasor" is aware. Gross negligence usually bars limitations of liability in contracts. Such contracts may include exculpatory clauses, which bar suit in cases of simple negligence. These are generally held to be valid, but instances of gross negligence are found to be in violation of public policy and are, therefore, not enforceable.

Promissory note—a written promise to pay a specified sum of money to another at a specified time. It is an unconditional promise to pay. Promissory notes are often used to obtain payment from employees caught stealing from their employers.

Public policy—public conscience and morals that are applied throughout the community. Supported by public opinion, public policy relates to those matters that promote the general health, welfare, and safety of all persons. Public policy consists of those tangible, noticeable duties that each man must extend to his fellowmen.

The *public policy doctrine* affords courts the right to refuse to enforce contracts that violate the law or public policy.

Qualified immunity—an affirmative defense to civil prosecution held by public officials. Qualified immunity is extended to governmental agents so that they may exercise discretionary authority. They are immune to prosecution if their actions did not violate statutory laws or constitutional safeguards. Government officials acting with probable cause cannot be held civilly liable.

Reasonable and due care—that degree of a care that a reasonably prudent person would exhibit in similar circumstances. The degree of care is necessary to prevent an action of negligence.

Reasonable belief—facts sufficient to cause a reasonable and cautious man to believe that a certain set of circumstances is true, such as that a person committed a felony.

*Recovery, for bat*tery, false imprisonment, false arrest, malicious prosecution, wrongful death. or claims for forfeiture the amount of damages awarded to the plaintiff. The restoration of a right to an aggrieved party accomplished by the judgment of a court (damages, injunctive relief punitive damages).

Statute of limitations—in Pennsylvania, the limits vary between torts; actions must be filed within one year for libel, slander, or invasion of privacy. The limit extends to two years for assault.

Strict liability—liability without fault, also known as "absolute liability." Defendants can be found liable for harm caused by impurities in foodstuffs, the acts of wild animals, the employment of explosives without regard to protective measures taken. The courts view such activities so inherently dangerous that the individual engaging in them is strictly liable for any harm caused to third parties. Strict liability also applies to criminal law. Strict liability crimes are those offenses where the elements of the offense do not contain intent. Examples would be speeding, drunken driving, or the release of toxic chemicals into the environment.

Substantial evidence rule—substantial evidence that a fact is true is sufficient to let stand an administrative agency ruling by a court reviewing that ruling. Under the rule, evidence is competent and may be considered regardless of its source, if it is reasonable to support a conclusion. Substantial evidence is more than a mere scintilla, but less than a preponderance.

Summary judgment—a decision rendered by a court when there is no dispute as to the facts of a case and there is only a question of law to be addressed. Summary judgments allow the expeditious handling of civil complaints whereby one party believes it will prevail as a matter of law. This party makes a motion for summary judgment.

Arrest and Detention

Arrest—Depriving a person of liberty by legal authority in order that he may answer to a criminal charge. Generally, citizen's arrest can be performed for the following reasons—*which vary considerably from state to state:*

1. Commission of a felony
2. Felony committed in arrestor's presence
3. Felony witnessed by arrestor
4. Breach of the peace resulting from a felony or misdemeanor being committed

Most jurisdictions require that a felony has been committed in fact, that the person making the citizen's arrest has reasonable grounds to believe the person being arrested has committed the felony, and that the felony was committed in the arrestor's presence.

There are also specific circumstances under which certain persons may make arrests in various states. As an example, in Pennsylvania, a train car conductor may make an arrest of a person carrying a bomb on a train.

Citizen's arrest is not looked on favorably by employers or the courts as there is often no privilege or *qualified immunity* from civil prosecution for private persons. While police officers who have *probable cause* are immune from civil actions due to false arrest, private persons are not. Additionally, if the arrest made by security is invalid, the police officers are not obligated to take the arrestee into custody. This makes a very troublesome situation.

Arrest Procedures

- Notify the arrestee of the purpose of the arrest.
- Be certain to use only reasonable or necessary force.
- Restrict searches of arrestees to cursory crushing of the outer clothing for weapons using the fingerprint area of the hands (preferably protective gloves should be worn).
- Do not keep the person in custody any longer than is necessary.
- The police should be notified as soon after the arrest as possible and the arrestee should be delivered to the police without delay.

Juveniles

Juveniles being arrested or detained give rise to special problems. Many states have complicated and changing rules concerning juveniles. In general, the protection officer should bear in mind the following when taking a juvenile into custody:

1. Consider legal relationship to juvenile—in *loco parentis* ("in place of the parent") exists when a person assumes temporary supervision of a child in the absence of a parent. An example would be teachers at schools.
2. Know and follow all state laws—these vary *considerably*!
3. Notify appropriate authorities—police, juvenile probation, truant officers.
4. Notify parents or guardians.
5. Release to parents (summary offense or civil recovery), police, or juvenile authorities at earliest opportunity.
6. Children under 7 years of age cannot be taken into custody for a crime.

Detention

Detention is the act of temporarily stopping someone's freedom of movement. This may be done to protect oneself or another whom the officer has a *duty* to protect against an assault, to stop a trespasser, to conduct an entry or exit search, or to recover merchandise. Detention could result in arrest, but in the overwhelming majority of cases it is not performed with the intent of bringing someone before a court. Generally, detention does not involve the use of force and should not involve the use of force if at all possible. Detention authority is specified in state statutes regarding shoplifting and library theft, but most states— *and legal texts*—are mute on the subject when applied to the more common performance of detention at entry points, in schools, in high security facilities, etc.

Merchant's privilege statutes vary considerably between the states. *Generally* they extend qualified immunity that allows merchants, their employees, or agents to take persons into custody with *probable cause* (sometimes this is referred to as "reasonable cause") that the person has committed a retail theft for the following purposes:

- To request and verify information.
- To ascertain if the person has unpurchased merchandise in his or her possession.
- To inform a peace or police officer of the detention and surrender that person to the officer.

The following points serve as evaluative tools by which protection professionals can assess detention practices:

1. Know and articulate specific purpose of detention—self-defense, recovery of merchandise, protection of others, prevention of trespass, etc. Officers must be able to clearly state why they are restricting someone's freedom.
2. Have a written policy on detention that is implemented via specific procedures, post orders, etc.
3. Develop policy after assessing state statutes, regulatory requirements, case law, and local law enforcement agency procedures.
4. Know the policy and operating procedures of responding law enforcement agencies. These vary from place to place and impact what security departments do regarding detention.
5. Call police as soon as possible in those cases requiring their assistance—where persons are violent and/or where criminal charges will be brought against someone.
6. Record the times of calls to the police, the results of such calls, and the arrival times, numbers, and names of responding police officers.
7. Use effective and legally correct (truthful, accurate) verbalization when detaining. Avoid bluffing.
8. Tell the detainee what is transpiring, but no more than is necessary. Provide a basic explanation, but do not engage in protracted dialogue about the reason, the officer's authority, etc. Lengthy discussions create room for argument!
9. Be as polite and considerate as possible to the detainee. Scrupulously avoid referring to them in demeaning terms. Remember the adage "respect begets respect."
10. Assess the detainee and environment for safety—avoid areas with a lot of glass, easy access to weapons, hazardous materials, or the inability to secure the room from associates of the detainee—before initiating the contact.
11. Avoid physical contact and document in detail *any and all* physical contact that occurs.
12. Understand the relationship of the detainee to your employer as much as possible. An employee can be spoken to longer in the eyes of the courts as they are being compensated for their time via an established business relationship.
13. Detain in a safe, secure area under your control. Control is the issue. Whose "turf" the detention occurs on will play a large role in determining which area to use.
14. Detain in a private place. A quiet, somewhat secluded, comfortable office environment is best to minimize interpersonal tensions between the officer and detainee. A private setting also helps to preclude any embarrassment the detainee may feel.

15. Have witnesses to the detention the same sex as the detainee.
16. Search the detainee in an appropriate manner: visual scan, cursory search for weapons, consent search of purse, etc. Employer policies will dictate the type and nature of the search. Officers should always have some reasonable degree of assurance that the detainee is not armed.
17. Restrain the detainee in an appropriate manner; have them sit with hands in view, handcuff, four-position restraints, etc.
18. Separate detainees from each other.
19. Question detainees for basic information and record their statements. Ask their names, purpose for being in the area, their identification cards, etc. This is basic information rather than an interrogation with the intent of obtaining statements suggesting guilt by the detainee.
20. Debrief the detainee as appropriate by complimenting them, explaining the impropriety to them, getting their acknowledgment of their inappropriate actions, etc.
21. Document the detention completely, being sure to include all statements, admissions, threats, etc.

Considerations Regarding the Use of Force

The lawful—and *safe*—use of force by private security personnel is a growing concern. Private security personnel are apt to encounter aggressive and potentially violent individuals in shopping centers, theaters, restaurants, amusement parks, "gated communities," and other places. In such environments, security personnel are largely taking the role of the old time cop on the beat in a downtown urban environment. As there is more privatization of protective services in courthouses, municipal buildings, public parks, municipal garages, and housing projects, so too the potential for use of force encounters.

Use of Force Continuum

Developed by Dr. Kevin Parsons, the Use of Force Continuum is a guide to using only that degree of force necessary to effect the immediate purpose for its employment. Other continuums have been developed by PPCT Management Systems, Larry Smith Enterprises, the Federal Law Enforcement Training Center, Calibre Press, and other organizations. All of them consist of a series of logical steps toward escalating the level of force used against an assailant. Officer presence would be followed by verbal controls, which would be followed by soft empty hand control. After, this would be striking with the hands, impact weapons, and, finally, deadly force. Note that there are differences of opinion among the experts regarding these continuums. Also note that the particular circumstances involving the use of force vary from situation to situation. An untrained officer using a lateral vascular neck restraint is a far cry from a trained and proficient individual employing the same technique. Similarly, the modification of any weapons used will change their place on the continuum. Adding CS or CN agent to oleoresin capsicum ("pepper spray") will change the content and effect of the aerosol. This is one reason why modifying weapons is generally a bad idea.

Deadly Force

That force which is readily capable of causing death or *serious bodily injury*. Deadly force can never be used if the possibility exists that you can retreat without injury to yourself or others.

Serious Bodily Injury

Bodily injury which creates a substantial risk of death or results in permanent disfigurement, or the protracted loss of use of any bodily member or organ. Sometimes this is called "great bodily harm."

Evaluating the Use of Force

The following are some basic standards that courts use to evaluate the use of force by police and security personnell: This is basically the definition of assault. The officer must be under assault to use force, except when arresting someone.

Ability—Does the assailant have the ability to cause bodily harm to the officer or someone he/she has a duty to protect?

Manifest intent—Has the assailant shown by his/her actions, an intent to harm the officer?

Imminent Jeopardy—Does the officer or others whom the officer has a duty to protect feel threatened, fearful or scared of being seriously harmed based on the assailants show of intent to act.

Consider Alternatives—Is the officer precluded from using force by taking some *alternative* action such as verbal persuasion, hard verbal commands, retreating, or the use of a lesser degree of force? As almost all encounters with persons do not call for the use of force, some attention to supportive communications is in order:

a) Honor subject's personal space.
b) Introduce yourself.
c) Employ *active listening* techniques.
d) Use "we" rather than "you," which tends to be accusatory and inflammatory.
e) Have subject sit down.
f) Offer subject something to drink—other than hot coffee or alcoholic beverages!
g) Ask open ended questions, which require some explanation by the subject,
h) Use *paraphrasing* and *reflection* to clarify what the subject says.
i) Beware of your fears and prejudices!

Some questions the officer can use to determine what, if any, force to employ in a given situation are as follows:

1. Am I in *imminent physical jeopardy?*
2. Is someone whom I have a *duty* to protect in *imminent physical jeopardy?*
3. Is my mission in jeopardy—preventing trespass, protecting assets from destruction, preventing theft, maintaining order, preventing escape?
4. Do I have another *alternative*—persuasion, "hard" verbal techniques such as screaming, retreat, subsequent criminal, or civil redress—to using force?
5. How will my actions be viewed by others—supervisors, police, courts, the public/community—who may evaluate them?
6. Preclusion—If the officer has no alternatives to use of force he/she is said to be in a state of preclusion. Preclusion must be present in each use of force when dealing with assailants.

Specific Circumstances

There are certain state statutes that enable private persons to use force in specific situations such as mental health commitments, in schools, where required by law to maintain order, where persons are assembled, etc. These statutes create both a legal justification for the use of force and a professional obligation. The obligation is not to be taken lightly! Officers should become familiar with local laws regarding this.

Juveniles

Also, there are varied standards for using force when juveniles are involved. In many cases, these statutes relate to the arrest of juveniles. State statutes on juveniles should be read and studied by those in the business of protection or teaching protection officers!

Postevent Actions

Much of the legal and public/community relations difficulty associated with the employment of force occurs after the incident. Unprofessional behavior after an encounter with an aggressor can sway the verdict in both the legal system and the "court of public opinion" against the officer involved. This may be true even if the use of force was appropriate. For this reason, extreme care must be taken following a use of force encounter. Complete documentation of the incident and control of statements and media coverage is crucial! At a minimum, the following should be recorded in use of force situations:

- Complete, *professional* description of subject's aggressive behavior. This includes verbal *and* nonverbal behavior. It must include all behaviors that lead to the employment of force against the subject.
- Complete, *professional* description of officers' actions to control subject.
- All witnesses and *points of contacts* such as home and work phone numbers, email, addresses, etc.
- Listing of *all* persons who assisted and responded to the incident. Often witnesses recall seeing a large number of security and/or police officers at the scene of a fight. The perception is that a large number of officers were using force against the subject. In fact, most of the "uniforms" present have arrived after the incident is over. Unfortunately, witnesses—and cameras—see a lone subject being overwhelmed by "an army" of officers. Care should be taken to specify the arrival time of each officer as best as can be done. Obviously, video of an event provides a record and the chance to examine what occurred (this may be a sound argument for installing surveillance cameras in certain locations).
- Description of medical care given—note that the officer has a *duty* to provide medical care to an assailant. Information on ambulance response time, hospital care and any, and all medical care given should be noted. If medical care is offered and refused, this should also be noted.
- Chronological detailing of facts, leading up to the most aggressive actions by the subject. This will "walk the reader" through the scenario so that he/she can completely understand it. Note that a good report is one that enables the reader to feel almost as if they were at the scene of the incident.
- Factual agreement between all accounts!

Media and public statements should be minimized. Statements to the media should only be given by a designated media representative. Statements by the officer should not be given to *anyone* except his or her supervisor and/or attorney. These persons should be briefed as soon as practicable. THE MORE THE OFFICER CAN BE KEPT AWAY FROM THE PUBLIC AND THE LESS HE OR SHE SAYS, THE BETTER.

Civil Liability

Civil law impacts on the actions *and* inactions of protective forces each and every day. The potential liability of being sued—having to pay attorneys and spend an extensive amount of man-hours on the case—mandates that circumstances that could create lawsuits should be discovered and avoided! Should a suit make it to court (out-of-court settlements are given by the defendant in 90% of the cases) and the plaintiff prevails, the potential of having to pay plaintiff's legal fees, compensatory damages and possible punitive damages raises the stakes even further.

Intentional Torts

Assault

- An intentional act causing an apprehension of imminent physical contact.
- No contact must be made.

Battery

- Unconsented, unlawful touching.
- No apprehension of touching necessary.
- Any degree of physical contact can be battery.
- May also include causing contact with the person by his or her clothing such as knocking off someone's hat.

False Arrest

- Unlawful restraint of another.

False Imprisonment

- An act that completely confines a plaintiff within fixed boundaries.
- An intent to confine.
- Defendant is responsible for or causes the confinement.
- Plaintiff was aware and knowledgeable of the confinement or was harmed by it.

Defamation

- False accusations.
- Injury to another's reputation.
- Can be written (libel) or spoken (slander).
- Accusation of commission of a crime is defamation per se.

Invasion of Privacy

- Unlawful, unreasonable intrusion on another's privacy.
- Can be physical or mental privacy.
- Can include unconsented publication of a private fact to a third person.

Malicious Prosecution

- Bringing or *pursuing* groundless criminal charges against another.
- Lack of probable cause is the key.
- Criminal proceeding terminates in favor of the defendant.

Negligent Infliction of Emotional Distress

- An act that is deemed extreme or outrageous.
- The intent to cause another severe emotional distress.
- Actual suffering of severe emotional distress.
- Causation—defendant is the actual cause of the emotional distress.
- May need to be caused by physical contact—this is now a minority view with the contiguous test.
- Can be limited as a *parasitic* action in that it must follow another tort action such as assault, defamation, etc. Whether this is true in a particular state, infliction of emotional distress does give the plaintiff another avenue of recovery.

Conversion

Wrongful appropriation of the property of another. Depriving the owner of the property for an indefinite time. Altering something or exercising control over something so that the owner's rights are excluded. Conversion is the civil aspect of theft.

Wrongful Discharge or Termination

An action by an at-will employee alleging that the employer discharged the employee in violation of a law or a contractual agreement. This tort is growing and the at-will doctrine

is rapidly dissolving. An employment at-will protection of the defendant is reduced or eliminated by the following factors:

- Contractual relationships that have been established—any violation of the terms of the agreement by the employer would enable the employee to bring an action for wrongful termination.
- Public policy (a state or federal statute) such as ADA or various whistle-blower statutes that have been enacted by both the federal government and many states. An example of this would be an employee in an OSHA-regulated workplace lodging a complaint with the Administration concerning a safety violation.
- An implied employment contract where promises were made to the employee ("You'll always have a job here as long as you want one").
- An implied covenant of good faith where the employer must behave honestly and conscientiously. If trickery, deceit, or duress is applied to the employee, there may be grounds for a wrongful termination action.

In some cases, parasitic actions for emotional stress are filed due to the loss of the job, status, and income. Depending on the jurisdiction, these charges can add substantially to the amount recovered by the plaintiff.

Negligence

Negligence actions can easily be lodged against an organization. In some cases, managers can be held *personally liable* for their negligence. Negligence is failing to prevent loss/harm/injury when there was a duty owed to the plaintiff and *reasonable and due care* would have prevented the injury from occurring. In essence, negligence consists of five elements:

1. The existence of a duty as established via law or contract.
2. A failure to perform that duty.
3. Harm or injury to a party to whom the duty was owed.
4. The harm was reasonably foreseeable.
5. The harm was caused by the failure to perform the duty.

One aspect of liability is suits based on the principle of respondeat superior ("let the master answer"). This means that employers can be held liable for the actions of their employees that are committed within the scope of employment. Scope of employment is generally defined by:

1. Time—was the employee on-duty when the action occurred?
2. Place—was the employee on employer's property at time of offense?
3. Purpose—was the act committed in furtherance of the employer's interests?

Other sources of liability can accrue if the employer was negligent—*failing to take reasonable and due care to prevent a foreseeable injury that he had a duty to prevent*—in any of the following areas:

1. *Selection*—hiring someone without properly screening them and placing them in a position of trust (accountant) or where they have access to keys (maintenance personnel in apartment complexes or schools) or where others may be exposed to dangerous propensities that they may have (convicted pedophiles in day care centers or convicted rapists in colleges). Access to personal information or financial accounts should also be seriously considered when selecting an employee; violence is not the only threat.
2. *Retention*—continuing the employment of someone with whom the defendant knows or *should have known* has dangerous proclivities.
3. *Entrustment*—entrusting a dangerous item to another whom the provider knew, or should have known, is likely to use such item in a reckless manner likely to cause harm to others. This could be a driver of a vehicle or the arming of a protection officer who has been known to be untrustworthy of handling a weapon. Obviously,

state licenses and certifications in the use and carrying of weapons are important to acquire and maintain.
4. *Supervision*—not properly supervising personnel in situations where someone suffers injury due to the failure. This could include having an inadequate span of control or an absence of supervisory checks.
5. *Instruction*—failing to properly direct a subordinate so that a third party—or the subordinate—suffers harm.
6. *Training*—failing to properly train someone to perform job duties with the result that an injury is caused.

Some basic questions that should be addressed in suits regarding training liability are:

1. Was the employee given instruction in the area at issue?
2. What type of instruction was given—video, manual review, lecture, etc?
3. What type and how much practice was the employee given to ensure task proficiency?
4. For emergency skills, what type and frequency of refresher training was given?
5. How was the learning tested or evaluated?
6. What were the qualifications of those giving the instruction?
7. Are there recognized instructional standards for the area of instruction, such as certifications?
8. Are there statutory (state or federal laws) or administrative/regulatory standards (OSHA, Department of Energy, etc.) regarding the area of training?

Independent Contractors

These are individuals or firms who/that perform work for the principal (client) but the principal does not have control over them. The principal is not vicariously liable for the acts of an independent contractor except in the following circumstances:

1. The activity being carried out is inherently dangerous.
2. The activity is personal in nature and thus nondelegable; safety and security functions are often found by courts to be non-delegable.
3. Ratification of the act by the principal occurs.

Section 1983 and 1985 Actions

The Ku Klux Klan Act of 1871 was enacted to ensure the fourth Amendment rights of recently freed slaves in the southern part of the United States. A portion of the Act, Title 42, Section 1983, provides for civil redress in federal court for those person whose fourth Amendment rights are infringed on by those acting *under color of law*. Section 1983 provides an *additional remedy* for tortious conduct within the federal court system.

> *Every person who, under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory, subjects, or causes to be subjected, any citizen of the United States or other persons within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, suit in equity, or other proceeding for redress.*

A few key points concerning Section 1983 actions are:

- The defendant must be acting under color of law.
- Private corporations cannot be held *vicariously liable* for the actions of employees.
- Private party defendants cannot assert *qualified immunity* defenses to suits as can publicly employed police officers.
- Private corporations can be held liable for attorneys' fees in 1983 suits if they employ a public (off-duty) officer.

Section 1983 actions will probably escalate with increasing privatization and closer relations between police and security organizations. Additionally, *criminal penalties* may

be imposed in certain circumstances for civil right violations. Title 18, United States Code, Section 242, provides for criminal prosecution for anyone who, under color of law, statute, ordinance, regulation or custom, willfully subjects an inhabitant of any State, Territory, or the District of Columbia to the deprivation of any rights, privileges, or immunities secured or protected by the Constitution of the United States, or to different punishments, pains, or penalties, on account of such an inhabitant being an alien, or by reason of his color or race, than are prescribed for the punishment of citizens, shall be fined not more than $1,000 or imprisoned not more than one year, or both. If bodily injury results, they may be subject to 10 years imprisonment. If death occurs they may be subject to any term of years or for life.

Section 1985 of 42 USC provides for recovery by plaintiffs where a *conspiracy* exists to deprive someone of their rights, privileges, and immunities secured by the Constitution and laws of the United States. Two or more persons planning to deprive someone of their rights may be prosecuted under Section 1985. With the increased use of investigative task forces, the potential for 1985 actions increases.

Strict Liability

Strict liability is applied in cases where there is no intent to cause harm or injury; the act itself is ultrahazardous. It is dangerous enough to cause unconditional or *absolute* liability. Activities that qualify for strict liability include:

- keeping wild animals
- using explosives
- underwater gear
- firearms in some cases
- "Certificates of Authority" issued by government agencies to private entities may also create absolute liability

Criminal Law and Criminal Liability

Criminal law is of obvious import to protection professionals who generally deal with a limited set of behaviors (crimes) within their respective work environs. Security personnel must be knowledgeable of these offenses. They must know the elements of each and must be skilled at prosecuting each. Note that aside from the obvious benefit this knowledge has in terms of job proficiency, it is also essential for avoiding liability and preserving good relations with law enforcement and local district attorneys. Police should be called to make valid, "solid" arrests. The officer calling should know the elements of the offense in question to make the police officers' job easier.

Another issue is with new or unique offenses. Sometimes new laws are written and police are uncomfortable enforcing them. Protection professionals should attempt to learn as much as possible about the new laws. They may have to seek legal counsel or meet with prosecuting attorneys to understand the nuances behind the new legislation. They should also be knowledgeable of other offenses that the defendant may be charged with during the same course of conduct. Examples of these would be indecent or sexual assault in cases of rape, receiving stolen property in cases of robbery or burglary (the perpetrator had stolen property from his or her person), conspiracy in cases regarding controlled substances.

Trespassing

Model Penal Code, Section 221.2

1. Buildings and occupied structures: A person, knowing that he/she is not licensed or privileged to do so, enters or surreptitiously remains in any building or occupied structure, or separately secured or occupied portion thereof.
2. Defiant trespassers: A person knowing that he/she is not licensed or privileged to do so remains in any place in which notice against trespass is given by:
   - Actual communication to the person.

- Posting in a manner prescribed by law.
- Fencing or enclosure manifestly designed to exclude intruders.

3. Defenses: Affirmative defenses for charges under this section are as follows:
   - The building or occupied structure involved with a trespassing offense is *abandoned*.
   - The premises, at the time, were open to members of the public, provided that all lawful conditions pertaining to access have been complied with.
   - The trespasser believes that the owner would have authorized his/her presence there.

Dealing with Trespassers

Protection officers are often called on to evict persons from the property they are hired to protect. Performing this function can involve a host of difficulties that are generally not foreseen by property managers. Property/facility managers simply desire a certain "culture" or ambience within the boundaries of the facility or property. They leave the details to the protection officers as to how to be the "preservers of the corporate culture." Such a role is complex and challenging. How effectively the protection officer can secure the property he/she is employed to protect will determine the degree of legal, operational, and safety problems that are confronted. For these reasons, evicting trespassers should be done *professionally*. Below is a list of recommended practices for controlling trespass to property.

1. A polite request to leave should be employed. This can be prefaced with an interview as to what the person is doing so as to better assess the situation. Persons will not have to be evicted in every case; some will simply comply with the protection officer's request.
2. Conduct the process in private as much as possible to preclude acting-out behavior in front of an audience as well as to avoid exposure to defamation/invasion of privacy actions.
3. Avoid invading the personal space of the evictee! A respectable distance—at least a leg length—must be maintained *at all times*. When there are indications that the person is violent, this distance should be increased to at least 10 ft. Care should be taken so as not to corner the person when first approaching them or going through a doorway. The latter scenario is a common cause of aggressive behavior when evicting someone from a room.
4. Accompany the evictee all the way off the property so as to monitor and influence their behavior. Being too far from the evictee can make them feel unsupervised and rebellious. Acting-out behavior, such as shouting, cursing, and threatening, is likely to escalate. Aside from being detrimental to the decorum, this behavior can incite problems from nearby crowds of people.
5. Document the action in a daily log, etc. This lists the basic information regarding a routine eviction. Should there be a substantial problem or the person being evicted has been a problem in the past, a complete incident report should be prepared. Also consider video, still shots, and audio documentation.
6. Evict with a partner/witness. Security officers can use the "Contact/Cover" concept where one officer communicates with the subject and the other oversees from an appropriate distance/location for safety purposes.
7. Obtain police assistance if force must be used. Advise police of the problem when calling them. If the person has been violent, threatening, or has caused prior disturbances, the police should know this. Police may also be amenable to escorting persons off the property who have been given trespass notices.
8. Advise the resistant person of the legal consequences of his/her actions—a trespassing charge as well as any other appropriate charges. Knowledge of the law serves to establish the officer's professionalism and authority; few persons will argue if the officer knows what he/she is doing. Legal knowledge also helps to maintain a positive relationship with local police!

9. Use the phrases "private property" or "_____ (company, college, hospital, etc.) property." Most people have a degree of respect for private property, realize they are on someone else's "turf" and comply with reasonable directions. Even chronic troublemakers are thrown off guard by the phrase "private property."
10. Give persons being evicted very specific parameters as far as time limits, routes to take, etc. Be fair and firm with this. Document it.
11. Enforce only lawful and *reasonable* rules. If the rules are not clear and concise, do not attempt to enforce them! Ambiguous, unenforceable rules will lead to trouble with police after they are summoned to arrest a trespasser and do not feel obligated to do so. Such encounters destroy the credibility of security, management, and the police.
12. Consider utilizing prepared notices on company letterhead to mail as certified or registered letters. Such trespass letters should specify the unauthorized activity and dates of occurrence. In public places such as shopping centers, there should be several instances of arrests and evictions indicated as the person is being banned from a whole host of retail establishments. Prepared in a slightly different format, these can also be handed to trespassers. *The Retailer's Guide to Loss Prevention and Security* by Donald Horan from CRC Press (800/272-7737) provides an excellent discussion of both trespass procedures that can be applied to a retail environment as well as some outstanding tips on establishing relationships with law enforcement agencies.
13. Provide the trespasser with the option of behaving or leaving and document that this was done. The trespasser made the decision to remain on the property.
14. Discuss with police and other parties such as managers after they have evicted or arrested persons how to improve on the process. Make sure that everyone can share perspectives on the process!

Eviction of trespassers is a challenging undertaking which must be professionally handled in order to ensure that civil rights, property rights, and the appropriate rules/culture/decorum are preserved. *Management representatives*—protection officers—who serve as *the ambassadors of the organization* can do no less.

Labor Law, Discipline, and Dismissal

As security personnel are the representatives of their employers, they serve as liaison between employees and management. Whether these employees are line or managerial level personnel, there are certain legal and ethical standards governing the employee–employer relationship. Labor law encompasses statutory law (legislation), administrative or regulatory law, contract law, civil law, court decisions, and a smattering of criminal law. Unfortunately, labor law has traditionally been overlooked in texts and courses for protection officers.

Employment-at-Will

Absent an express agreement to the contrary, either party may terminate the employment relationship. No cause must be shown. The employment-at-will doctrine is largely eroded. One problem is the myriad of state and federal employment laws; while an employer may believe that he can terminate an employee-at-will, there may be in existence—unbeknownst to him—a state or federal statute that prohibits such action. Aside from these specific exceptions, there are some general exceptions to the employment-at-will doctrine. Some of the more notable general exceptions are:

1. *Public policy*—not hiring or firing someone because they are on jury duty, in the reserves, etc. Another example would be not hiring or firing someone who has lodged a complaint with a state or federal agency against an employer. In this latter example, "whistle-blower" statutes *specifically* forbid discriminatory treatment of employees who file complaints.
2. *Good faith*—employers must treat employees in a fair, honest manner.
3. *Implied contracts*—promises made by employers must be adhered to. Promises can be made in job interviews, employee handbooks, memos, etc. A systematic review of employee handbooks and other orientation materials should always be conducted!

Wagner Act of 1935 (National Labor Relations Act)

- Created the National Labor Relations Board.
- Employers cannot interfere with efforts of employees to form, join, or assist labor organizations, or to engage in concerted activities for mutual aid or protection.
- Domination of a labor organization or contribution of financial or other support to it.
- Discrimination in hire or tenure of employees for the reason of union affiliation.
- Discrimination against employees for filing charges or giving testimony under the Act.

Court Injunctions

Injunctive relief can be obtained from the courts in labor disputes provided that the petitioner has complied with all lawful obligations and has taken reasonable steps to resolve the conflict through negotiation. In general, courts will issue restraining orders when they find that:

1. Unlawful acts have been either threatened or committed and will continue to be committed unless they are restrained by the court.
2. Damage of a substantial, irreparable nature will be done to the complainant's property.
3. The complainant will suffer greater injury by not having the order than the defendants will suffer by having it.
4. The complainant does not have an adequate remedy at law (civil or criminal).
5. Public authorities are unable or unwilling to protect the complainant's property.

Fair Labor Standards Act of 1938

Passed in 1938 to help pull the country out of the great depression by making employers hire more workers due to the overtime provision. It also helped to raise people's standards of living by requiring that minimum wages be paid. The Fair Labor Standards Act established the following:

1. Minimum wages must be paid to workers.
2. Wage and hour division of the Department of Labor.
3. Overtime pay at time and a half of the regular rate of pay—not discretionary pay such as merit pay, bonuses, etc.—must be paid for hours worked over 40 within one week's time.
4. Children younger than 14 cannot be employed save for children employed by parents, in agriculture after school, as child actors, or newspaper deliverers. Children younger than 18 are not authorized to work in hazardous occupations, as determined by the Secretary of Labor. Children older than 16 may be employed in nonhazardous work; 16 is the basic age at which children may work.
5. Retention of payroll, employment contracts, and collective bargaining agreements for three years. Time cards, earning records, overtime records, work schedules, etc. must be kept for two years.

"Hours worked" is any activity participated in that is job-related and benefits the employer. The employer must control the work; they must know how much off-duty work is being performed; if the work is not stopped by the employer, the employer must pay for it. Employees have no obligation to stop or control the work being performed.

Overtime exemptions under the Act:

1. The burden of proof for exemptions rests with management.
2. "High-level management" personnel are exempt from overtime pay. Job descriptions—*not mere titles*—that delineate the work being performed as managerial in nature are required.
3. Management personnel must be paid on a salary basis in predetermined amounts each pay period. Pay is unrelated to hours worked.
4. Compensatory time can be paid to employees with the following stipulations:
   - There must be an agreement with the union.

- Compensatory time is an "alternative currency" for wages and as such is equal to wages.
- Compensatory time cannot be controlled or restricted by management unless it is a serious business interruption.
- There can be no "use it or lose it" stipulation.
- On termination of employment, all compensatory time is cashed out at today's rate.
- Enforcement of the Act via the Department of Labor or civil suit involving:
  - Time and a half back pay for all hours worked.
  - Interest—liquidated damages—at double the principal.
  - Two-year statute of limitations is in effect.
  - Reasonable attorneys' fees.
  - Punitive damages if the employer discriminates against the employee for lodging a complaint.

Taft–Hartley Act of 1947

Taft–Hartley shifted the balance of power back toward management. It established a series of management rights and provisions for governmental control of unions. Note that in the United States, unions reached their zenith during 1946–1947. The Act provided that:

- Unions could be found to engage in unfair labor practices such as requiring excessive union fees, forcing an employer to bargain with an uncertified union, and forcing an employer to pay for services not rendered.
- Provided for back pay awards for employees who have been reinstated in cases of unfair labor practices.
- Removed supervisors from protection as employees.
- Removed closed shop agreements that required an employee to join a union *prior* to being hired. Note that some employers—particularly small ones in construction and the maritime industries—draft agreements with unions that require the employer to *offer* the union an opportunity to fill vacant work assignments.
- Provided for emergency intervention by the president in the case of strikes that threaten national security.
- Prohibited guards from belonging to the same unions as other employees.
- Established the Federal Mediation and Conciliation Service to help in the settlement of unresolved disputes.
- Permitted suits by and against labor organizations for violating labor contracts.
- Prohibited union officials from accepting money from supervisors.
- Extended coverage of the Act to employees of private nonprofit hospitals in 1974.

Landrum–Griffin Act of 1959

Continuing the trend set by Taft–Hartley; this Act established more controls over union activities including:

- Provided freedom of speech, equal voting rights, control of dues, increases, retention of the right to sue, and rights to copies of labor agreements under which they worked.
- Required financial disclosure by unions and reports by employees of financial transactions with unions.
- Required bonding of union officers and prohibited recently convicted felons from holding office.
- Made illegal "hot cargo" agreements wherein employees agree not to use nonunion goods.

Strike Surveillance

Section 158 (a) (1) of the National Labor Relations Act prohibits an employer from any activity that would interfere with, restrain, or coerce employees who are exercising their lawful rights of collective bargaining. Activities such as picketing, union meetings, or accepting handbills from union organizers are protected. As photographing and conducting surveillance

of people has an inherently intimidating effect, the National Labor Relations Board has ruled that surveillance of persons engaged in collective bargaining activity constitutes an unfair labor practice. Exceptions to this are when the activity being documented is unlawful or when the information being collected is to be used in a petition for an injunction.

- Firms should seek advice from legal counsel about conducting surveillance to be used at an injunction hearing. Such evidence should actually be used at the hearing.
- Surveillance should not be undertaken prior to thorough documentation of the activities of strikers.

Polygraph Protection Act of 1988

Due to increasing concern by liberal members of Congress—such as Ted Kennedy—that employers were encroaching on the rights of workers, Congress passed the Polygraph Protection Act of 1988. This debate had been going on for a period of years in Congress. While the various states had laws restricting the use of polygraph testing (e.g., in Pennsylvania, an employer cannot require a prospective applicant to take a polygraph examination), until 1988 the federal government had no laws regarding the use of polygraphs in employment. The Polygraph Protection Act impacts on commercial businesses—government agencies, school systems, and correctional institutions are not affected. There are also exemptions for businesses under contract with the federal government, businesses in counterintelligence, armored car companies, security alarm, or service firms or those firms that manufacture, distribute, or dispense controlled substances. The basic provisions of the Act are:

- Employers cannot suggest or require an applicant for employment to take a polygraph test.
- Employers can suggest—*but not require*—current employees to take polygraph tests.
- Employers can suggest employees to take polygraph examinations when the following conditions have been met:
  a) The request must be related to a specific, ongoing investigation.
  b) The employee must have access to the property, money, or area under investigation.
  c) The employer must have reasonable suspicion that the employee was involved in the incident under investigation.
  d) At least 48 hours written notice be given prior to the examination.
  e) The examination must follow certain procedures such as lasting at least 90 min.
  f) A statement must be read to the examinee that includes his or her rights under the Act.

Discipline

- Keep employee handbook current!
- Document all transgressions and advise employees of this.

Dismissal

- Ensure that there are clear policies regarding terminable offenses.
- Avoid telling employees that they will never be fired without just cause, as this can create an implied employment contract.
- Ascertain that all employer policies have been followed leading up to the termination.
- Select a neutral location.
- Have a witness who does not talk, only listens.
- Have a written termination notice that specifies all previous disciplinary problems the employer has encountered with the employee.
- Be lobjective and a good listener; do not argue! Minimize attempts at reasoning with the to-be-terminated employee who is probably too emotional to be rational.
- Provide the employee with a written notice of the termination.
- Avoid using ambiguous terms such as “layoff.”
- Avoid giving notice at the end of a work day, prior to a holiday, or when the employee has just returned from vacation.

Federal False Claims Act of 1863

This law was enacted during the American Civil War (1861–1865) to protect the Union Army from unscrupulous contractors who were defrauding the government. The Act provides for civil penalties of $5,000 and $10,000 for each false payment demand, bill, etc. In addition, the defendant is liable for up to three times the amount of damages the government suffers due to the fraud. Other provisions entitle "whistle-blowers" to receive between 15% and 30% of the amount that the government recovers.

Legal Standards Regarding Privacy

Privacy is a large and growing issue. Databases can be misused, private information can be disseminated, and serious problems can plague individuals. Identity theft, as an example, takes ~700 hours to correct once one has been victimized. There is a growing array of legal standards at both the state and federal levels, which protect the privacy of information. Some of these statutes require specific protection measures, some contain criminal sanctions. Below are a few of the more important ones in the United States of America.

Privacy Act

Enacted in 1974, the Privacy Act requires federal agencies to collect and maintain only necessary information about citizens. It specifies:

- Citizens can see, copy, and correct files kept on them.
- While there is no response time mandated by the Act, a reply in 10 days is customary in many agencies.
- Intelligence and law enforcement agencies can exclude entire systems of records from disclosure.

Freedom of Information Act

Passed to improve citizens' access to records kept by the executive branch of government. Records will be disclosed unless they fall into one of the following categories:

- information on litigation
- internal agency memos
- trade secrets
- law enforcement activities
- Central Intelligence Agency, (CIA) activities
- classified documents
- personnel, medical, or other files that are matters of personal privacy
- confidential government sources

All 50 states have set up their own version of open-records laws.

Fair Credit Reporting Act of 1970

The purpose of this act was to regulate the collection and dissemination of consumer credit information. Consumer credit information can be personal credit histories; the language of the 1997 amendment suggests that it also affects criminal backgrounds, motor vehicle checks, and other types of public record checks normally performed during preemployment screening of job applicants. Investigative reports such as reference checks with employers, neighbors, friends, and associates are also considered consumer reports if they are obtained from an organization in business to provide such information. It regulates businesses that assemble reports for other businesses, such as:

- credit bureaus
- investigative reporting companies

- detective and collection agencies
- lender's exchanges
- information reporting companies

The Fair Credit Reporting Act basically establishes the following rights of consumers:

- Right to notice that the information is being reported
- Right of access to the information contained in consumer credit reports
- Right to correct any erroneous information in consumer credit reports

Note: There are also state acts that regulate the collection and reporting of consumer credit information. These are generally more restrictive than the federal law.

Employee Background Investigations

As employee background investigations are commonly, and increasingly, being conducted; it is essential to do them in a lawful, ethical, and professional manner. The Fair Credit Reporting Act and other statutes help to govern the conduct of employee background investigations. The following points are relevant to the conduct of background investigations in any political jurisdiction:

1. The inquiry should be well rounded. It should examine various aspects of the applicants past that are job related. Criminal history should be checked in the applicant's home, work, and commuting jurisdictions as they may have been convicted of crimes in any of those areas. A prior employment check and a reference check should always be done.
2. The investigation should comply with accepted standards. The ASIS Guideline on background investigations is a good place to start.
3. The investigation's depth and scope should be commensurate with the position being applied for. Background inquiries have levels of inquiry, which vary according to the sensitivity of the position the applicant is a candidate for. Cashier at a fast food restaurant require local criminal history but not motor vehicles check or civil records. Manager may require a credit check, civil records, driving history, and developed references.
4. Advise applicants of the presence of negative information. Allow them a reasonable amount of time to refute an investigation that has an adverse effect on the applicant. There may have been mistakes made and applicants should be allowed to clear them up. Three to five business days should be sufficient. Also make it clear that the employer, not the reporting agency (private investigative firm, credit bureau), is taking the adverse action.
5. Keep the investigation focused on employment related issues. Do not stray off into a "witch hunt" or "fishing expedition" where non-job related information is uncovered. All inquiries must have clearly defined business objectives. Work history and references should always be checked. An employee who walks to work does not need a motor vehicle bureau check done on them. An employee who has no access to cash or financial transactions does not need a credit check performed.
6. Follow the "golden rule": "*Do unto others as you would have them do unto you*." If it seems unfair, don't do it.
7. Never violate any applicable legal standards, in spirit as well as in letter.
8 Notify applicants and obtain written consent before any inquiry is initiated. Even if not specifically required by law, gaining written consent sends a message to the applicant that the inquiry will be conducted in a serious manner.
9. Utilize professional screening services if outsourcing. There are firms that specialize in background investigation. They are proficient at it and may also be able to offer consultation on related human resource issues. Such firms also are more apt to comply with the Fair Credit Reporting Act and other laws. They are less likely to use illegitimate data from internet sources that are old or inaccurate.

10. Verify all information of a negative nature before taking any adverse action. Database information should be verified to original documentation. Background investigators have a duty to not harm others. Background investigations have enormous potential to do just that.

Health Insurance Portability and Protection Act

Enacted in 1996, Health Insurance Portability and Protection Act (HIPPA) essentially requires *administrative safeguards* of patient data such as policies, procedures, a designated person in charge of the protection program, security awareness programs, and continuous review of existing policies and procedures. There are also *physical safeguards* required such as access control, specifying appropriate workstation functions. In addition *technical safeguards* must be implemented such as controlling access of authorized personnel and software programs to electronic information systems that contain electronic personal health information, protecting patient information from improper modification or destruction, audit controls, etc.

The PATRIOT Act

On October 26, 2001, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act was passed (USAPATRIOT). The majority of the Act's provisions relate to measures designed to enhance governmental investigation and have a major, and sometimes controversial, impact on privacy. The Act will probably become more important over time as it relates to the investigation of electronic crimes. A few of the provisions that impact the security industry are:

> Title III, International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001 financial institutions establish programs to combat money laundering and identify terrorists who may be posing as customers. The Title also requires enhanced due diligence of financial transactions.
>
> Title X, miscellaneous has a variety of provisions including a feasibility study of using biometric scanning systems at ports of entry, limits on the issuance of hazardous material licenses, and contracting security services at US military installations.

Trade Secrets

Trade secrets are formulas, patterns, processes, devices, or compilations of information that are used in one's business to gain an advantage over competitors who do not have the information. A trade secret has continuous use in the operation of the business. Some examples of trade secrets are:

- processes used in manufacturing
- patterns for a machine
- lists of customers
- codes for determining discounts or rebates
- methods of bookkeeping

The basic elements of a trade secret are:

- It must be secret, not known to others.
- It must be used in the business of the owner of the secret in order to obtain an advantage.
- There must be continuous or consistent business application of the secret.

Not all information used in business is a trade secret. Some factors used in determining whether information constitutes a trade secret are:

- To what extent is data known to the outside world?
- To what extent is data known by the holder's employees?
- What type of protective measures has the holder taken to safeguard secrecy of the data?

- What is the value of the information to the business and the competition?
- How much effort and money was spent in developing the data?
- How easily could this data be acquired legitimately by competitors?

Administrative Law

Administrative agencies have been created to regulate both business and government so that rapidly changing technology can be effectively controlled. Administrative agencies have a tremendous impact on the day-to-day operations of a business—one that is substantially greater than that of the courts or legislatures. Agencies differ in their jurisdiction and authority. While most have some form of judicial review, some do not. Some agencies, such as the Nuclear Regulatory Commission (NRC), enforce their rules through an internal appellate process prior to external judicial review; others such as the National Labor Relations Board must have the courts enforce their orders. In general, administrative agencies have the following types of authority:

1. *Rule-making or quasi-legislative power* as enumerated in the enabling statute that created the agency.
2. *Quasi-judicial*. Agencies hold hearings that are not limited by the formal rules of evidence or procedure used in court. The hearings must follow due process, the agency's own rules and regulations, provisions of the Administrative Procedures Act, and the Fifth Amendment protection against self-incrimination.

Judicial review of an agency decision can occur. With some agencies this is more common than with others; largely this is determined by the agencies, enabling statute that specifies the amount of authority that it has. Other factors include the impact of its rulings; those with minimal impact are unlikely to be appealed to a court while those creating major financial burdens will be.

Some factors that a court will examine on review are:

- Whether the agency was empowered to act as it did.
- Whether the agency followed statutory procedures or its own published procedures.
- Whether the agency acted in an arbitrary and capricious manner.
- Whether the record shows at least some facts on which the decision could rest. *Substantial evidence* that a reasonable mind would accept to support a conclusion; somewhat less than would be required for a preponderance of evidence.

Judicial review of agencies is limited. Courts are reluctant to overturn agency rulings as the "doctrine of administrative expertise" decrees that the legislative body that created the agency determined that agency's expertise. Therefore, the agency should rule on matters it has expertise in rather than the courts:

- When the Administrative Procedures Act or the agency's enabling statute prohibits review.
- When administrative remedies have not been exhausted.
- When the party requesting the review has no standing.
- When the government is not subject to suit.
- When the agency has statutory discretion to act or not to act and has not acted.

Investigative: where the agency can investigate and issue subpoenas for persons to testify at hearings and to produce documents. Subpoenas are enforced by the appropriate court via contempt citations, fines, imprisonment.

Federal Agencies

- OSHA
- EPA
- FCC
- EEOC

- NLRB
- TSA
- NRC

State Agencies

- OSHA (CALOSHA in California, etc.)
- Human Relations Commission
- Department of Environmental Resources

Municipal Agencies

- Zoning Commission
- Board of Health

Because administrative agencies can fine, suspend, or revoke licenses to operate as well as sue, management is very concerned about compliance. Surviving an audit by a government inspector is important; learning an agency's rules, and the interpretation of them, is crucial to success for security managers. Federal agencies publish their rules in *The Federal Register* as well as via press releases.

Administrative Language

Administrative language is important for security managers to understand. When reading regulations, the meanings of the following key words must be kept in mind:

> *"Shall"*—this means "must." There is a requirement to do a certain thing. Managers must ascertain that every "shall" is complied with!
> *"Should"*—this means recommended. While not specifically required, today's "shoulds" can become tomorrow's "shalls." Additionally, auditors look more favorably on businesses that take the "high road" rather than those who merely do enough to get by.
> *"May"*—this means that the activity discussed is optional. It is completely at the discretion of the business, neither required nor recommended.

Audits

Being audited is a fact of life for most businesses and governmental units. While the points listed below relate to audits conducted by regulatory agencies, the same principles apply when being audited by an insurance carrier or professional accreditation body such as the International Association of Campus Law Enforcement Administrators or the Joint Commission on Accreditation of Healthcare Organizations.

The 10 Commandments of Winning Audits

1. *Have up-to-date documentation of the standards being audited against.*
2. *Understand the formal authority of the auditing organization.*
3. *Know the history of the auditing organization.*
4. *Know and appreciate the philosophy of the auditing organization.*
5. *Assess the background and perspectives of the individual auditor.*
6. *Assess probable areas of specific inquiry and develop retrievability of data to match the inquiries.*
7. *Neatness/image is everything!*
8. *Use the language of the auditing entity.*
9. *Educate all personnel in the organization about the audit process.*
10. *Internalize the audit process—seek out suggestions from the auditing organization and develop internal audits.*

Interrogation

Interrogation—focused interviewing—is often performed by protection professionals. Sometimes this is done as part of an investigation and is a planned activity; sometimes it is rather spontaneous, such as, when catching someone in the act of commission. Whatever the case, interviews must be held that are free from duress and coercion of the subject. The resulting admissions, statements, or confessions must be valid!

The following cases address interrogation by private security personnel:

Miranda v. Arizona (1966) required that before police interrogate a person they have taken into *custody* or deprived of his freedom in any significant way, they must provide the following warnings:

1. You have the right to remain silent.
2. Whatever you say may be used against you.
3. You have the right to a lawyer.
4. If you cannot afford a lawyer, one will be provided to you.

Interrogation under Miranda may only proceed after the suspect makes a "knowing and intelligent waiver" of his rights. This should be in writing!

Security personnel, operating as security personnel, free and clear of government direction or control, are not obligated to give Miranda warnings in most states (California and Montana being exceptions). Security personnel acting in furtherance of a government interest would be subject to Miranda as well as all other constitutional protections.

Garrity v. New Jersey (1967)—employers cannot require employees to give statements regarding disciplinary matters and then use them in criminal prosecution. Employees giving statements that might incriminate them should note that the statement is being given pursuant to an employer's directive and cannot be used in a criminal action.

Weingarten v. National Labor Relations Board (1975)—employers who have entered into collective bargaining agreements with employees and are interviewing employees in a situation where the employee *reasonably believes* disciplinary action could result must:

- inform the employee of the time, place, and nature of the interview
- allow the employee representation by a union steward or interested coworker—*not an attorney*—at the meeting *if it is requested*

Employers are *not* required to:

- advise employees of their right to representation
- bargain with the representative
- suspend the interview if the representative is not readily available

Key Points on Interrogation

- Review case thoroughly—know as much as possible about both the event(s) and subject.
- Keep the interrogation in a private setting. This precludes publication of private information such as accusations. There may be another investigator, supervisor, union representative, or same-sex witness present, but privacy is the key element. Each person in the room should have a legitimate interest in the case. They must be there for a reason!
- Try to be as non-accusatory as possible.
- Make no promises that can't be kept, such as promising not to prosecute criminally if restitution is made.
- Keep statement preambles short—a few words to the effect that the statement is "free and voluntary" are sufficient. Avoid "policespeak" jargon, which is complicated and, in almost all cases, convoluted and confusing to the reader.

- With procedural violation statements, be sure to include sufficient biographical and work history data to indicate the employee's level of training and experience so that they are accurately depicted as untrained (didn't know any better) or were trained (knew better) and are subject to disciplinary procedures.
- Make sure that the statement is given free of duress and is in the subject's own words.
- It may be advisable for the investigator to write the statement with the subject; in this way, words and phrases that establish the key elements of culpability can be put into the statement.
- Be aware of—and scrupulously follow—any state laws regarding juveniles. Generally this means having the parents or guardians involved. Giving the parents/guardians time alone with the juvenile and then starting the interview may be the appropriate course of action.

Search and Seizure

Search and seizure by private persons is not normally controlled by the Constitution. Exceptions would be where a governmental interest or instigation was present. If government agents are directing the investigation then it is a government or state activity. Questions arise in those instances where there is government involvement but not specific direction. The following cases illustrate court decisions on searches by private parties.

Burdeau v McDowell (1921): the US Supreme Court found that evidence turned over to a government official by a private person could be used in prosecuting that person even though it was not seized within the confines of the Fourth Amendment. It also cannot be obtained by instigation of the government; the search must be performed for a private interest.

People v. Santiago (1967): a security officer arrested Santiago for shoplifting and subsequently searched Santiago's coat and found a loaded weapon. The search was contested on the grounds that the security officer didn't have the authority to search a person incidental to an arrest. The court found that the search was valid, as arrests made by citizens justify searches just as do those by government agents.

Many authors believe that a search of a suspect for weapons (frisk, pat down) can be performed by security personnel just as it can be by police who have reasonable suspicion to believe that criminal activity is afoot and that their *personal safety* is at stake. The justification of having no reasonable alternative to searching, so that personal safety—and the safety of others nearby—is preserved, should be present.

NJ v. TLO:—school officials and protection officers assigned to school environments may conduct searches of students if they have reasonable suspicion that the student is violating an administrative regulation of the school. Criminal behavior—in the above named case the possession of marijuana—can be prosecuted if discovered subsequent to an administrative search.

Simpson v. Commonwealth of Pennsylvania Unemployment Compensation Review Board: stipulated that an employer can suspend an employee for insubordination for refusing to submit to a search where the search was a recognized, posted procedure. The employee was not entitled to unemployment compensation during the period of his suspension.

Searches by private entities are often governed by collective bargaining agreements.

Employers should have a clause in their union contract that stipulates management's rights to search and investigate. Additionally, there should be published/posted notices of management's rights to search. *Maintaining* the right to search should be accomplished by conducting searches periodically, so as to keep the policy active.

Similarly, property owners can perform searches of persons entering or remaining on their property. These searches should be for specific, lawful purposes (combating the introduction of weapons or explosives or the theft of materials or equipment). They should be written into policy and specific procedures developed for their implementation. There should be notices posted regarding the search requirement. The example below might be appropriate for a museum or similar type of facility.

NOTICE: All bags must be checked. Receipts will be issued. Purses, briefcases, and other similar items are subject to search.

Additionally, the use of consent forms is suggested. If people are going to be given a hands-on search for weapons, they should sign a form giving their consent. Consent forms can be signed at the point of entry. Such forms can also include an acknowledgment of the rules for entering and remaining on the property. At a nuclear facility or R&D center, escort procedures would apply. Public events where people come into contact with VIPs and celebrities would also use consent forms containing an outline of entry rules.

Searches by private protection officers also are faced with the specter of civil liability. Obviously, tort actions for invasion of privacy, assault, battery, false arrest/false imprisonment, or negligent infliction of emotional distress can result from improper searches. Consent should always be obtained except in emergency situations or where an arrest is being made: if someone is assaultive, they need to be searched for weapons.

Evaluating Searches

1. What is the objective of the search—what is being looked for?
2. In whose interest is the search being conducted?
3. What is the searchee's reasonable expectation of privacy?
4. What is the written policy on searches?
5. What policy is being carried out in actual practice?
6. What has been the past practice in similar search situations?
7. How has consent been given? Is there actual consent or implied consent as a condition of employment or as part of a collective bargaining agreement?
8. Does the person giving consent have the authority to do so?
9. Is there an alternative to searching?
10. Should the search be performed by another entity?
11. Who is witnessing the search?
12. How is the search documented?
13. Will others who may see the search view it as reasonable?

Regulations Governing the Security Industry

There are various regulations that affect the security industry; most of these are at the state or provincial level. This is generally the case throughout North America as well as Europe. Some regulation is at the federal level. In general, states and provinces tend to regulate the following classes of personnel:

1. Armed security officers
2. Contract security service firms
3. Private investigators
4. Alarm dealers and installers

In some cases, polygraph operators and others are regulated by individual states. A continuous problem is that the state regulation is generally minimal at best. Another concern is that state regulatory bodies are usually made up of personnel from the law enforcement community who are not really security professionals and who often grant licenses to those who are in their network but make unreasonable demands on those who are not. An additional concern is having police-oriented instructors training security officers. The instructors may not know the culture of the security work environments. They may also look down on the "private security" personnel.

States such as California and Florida have extensive regulation of training for security personnel. These laws require 16 hours of preassignment training and an additional 4 hours of annual in-service training for unarmed officers. Armed personnel must also complete additional training. In Virginia, personal protection specialists (PPS) are required to complete a state-recognized training program. The most extensive regulation is Ontario's that takes the unusual step of requiring training for both contract and proprietary security personnel.

The federal government may or may not get involved in regulating security personnel. The most likely scenario would be for regulation of security service firms under contract

with the federal government. This may occur via individual contract on a piecemeal basis or through a legislative enactment. It is worth noting that there have been unsuccessful attempts to pass such legislation. Currently federal regulation is confined to:

1. Bank Protection Act of 1968
2. Transportation Security Administration (TSA) and National Transportation Safety Board (NTSB) security regulations
3. Nuclear Regulatory Commission (NRC) regulations
4. Department of Defense (DOD) security regulations for DOD contractors
5. Department of Energy regulations (DOE)

There is also a growing awareness on the part of Congress that private security personnel play a large and growing role in crime control. As the Department of Homeland Security matures there are also reports that indicate an awareness of the substantial role of private protection forces in security key aspects of America's infrastructure. In Canada, the Canadian General Standards Board has established regulations for security officers. Sometimes such legislation serves not so much to regulate directly as symbolically: subsequent laws, standards, and practices follow the original regulations to a large extent. An example of this would be the Bank Protection Act in the United States. Currently, credit unions are not covered by the Act's provisions but nonetheless have adopted them. The Bank Protection Act has, in effect, established an industry standard within the financial services community. It may be that it is possible to legislate morality—to some degree.

Standards

Standards are of extreme import in the arena of protective services. Standards are created by the surrounding community, the security industry itself, insurance organizations such as Underwriter's Laboratories or Factory Mutual, or professional organizations. Standards are important because they:

1. Provide a recognized level of excellence
2. Create a possible marketing opportunity for service providers
3. Establish what constitutes "reasonable and due care" in negligence cases
4. Mandate what measures must be taken per insurance policies

Standards are important to individual protective service careers, as compliance with standards is very important in certain industries. Healthcare facilities that don't comply with Joint Commission on the Accreditation of Healthcare Organizations security standards may lose JCAHO accreditation. This could mean the loss of federal grant monies.

Types of Standards

There are various types and sources for the promulgation of standards within the security industry. These can be broken down into the following categories:

Government mandated standards that are set by legislation—the Bank Protection Act, licensing laws for private investigators, local ordinances on false alarms, or the securing of parking lots. There are also those set by administrative agencies of the government—licensing *requirements* for security service firms, Physical Security Plan, and Contingency Plan mandates for US NRC licensed power plants. Government standards can also be set by nonadministrative agencies, such as the DOD mandates that DOD contractors must follow for the protection of classified information. In some cases, government agencies specify requirements that security service firms must comply with. They may require certain screening and training procedures in Requests For Proposals dealing with providing security to city, county, state, or federal property. Note that municipal standards such as robbery prevention measures in convenience stores or security practices at parking garages are being adopted throughout the country.

Community standards are those practices generally accepted within a geographical area. Examples would be the use of armed guards in shopping centers or CCTV in the lobbies of hotels or doormen in office buildings. In some cities this is common; in others it is

not. Community standards are not published or specified in any way. They are simply the operational norm within an area. A precise determination of them would require a survey of all similar environments in a specified geographical area.

Industry standards are generally accepted practices within an industry. These can be formally established through professional organizations such as the National Burglar and Fire Alarm Association or ASIS or can simply be those practices commonly followed within the hotel, shopping center, or telecommunications industry. *ISO 9000* standards can be thought of as industry standards regulating those businesses conducting foreign commerce. ISO standards contribute to making the development, manufacturing, and supply of products and services more efficient, safer, and cleaner.

Some of the standard setting organizations in the security industry are:

- *ASIS International* that has a variety of guidelines on such topics as Security Officer Selection and Training, Information Asset Protection, Business Continuity, Chief Security Officer (CSO), Preemployment Background Screening, Threat Advisory System Response.
- *NFPA* that develops codes on fire and electricity has established premises security standards such as NFPA 730 Guide for Premises Security. NFPA 730 covers construction, protection, occupancy features, and practices designed to reduce security vulnerabilities to life and property. NFPA 731 Standard for the Installation of Electronic Premises Security Systems covers the application, location, installation, performance, testing, and maintenance of physical security systems and their components. As NFPA is generally looked to by governments and insurance carriers as the standard setting organization, it can be anticipated that NFPA 730 and 731 will be adopted in municipal building codes and as specifications in insurance contracts. Over time this will have a very substantial impact on asset protection.
- *AAA* that sets standards for physical security of hotels and motels.
- *Building owners and managers association* that mandates construction specifications such as having handrails at a height of 34 in.
- *International association of campus law enforcement administrators* (IACLEA) who accredit college and university police, security, and public safety departments. The IACLEA accreditation standards are based on the Commission on Law Enforcement Accreditation (CALEA) where applicable. Standards unique to campus protection have also been developed. At one time IACLEA has crime prevention standards for college campuses but no longer publishes them.
- *International Association of Healthcare Safety & Security* has training standards for security officers and supervisors as well as specifications for healthcare security. There is also a safety training certification program for protection officers in the healthcare industry. The IAHSS training standard is well established within the healthcare industry; it dates back to 1975.

Giving Depositions and Testifying in Legal and Quasi-Legal Proceedings

Security personnel are often required to testify in disciplinary hearings for their employers, preliminary or probable cause criminal hearings, criminal trials, civil trials, hearings conducted by administrative agencies (unemployment, workers' compensation, OSHA), and labor arbitration. They are also often asked to give depositions in civil cases. Testimony is important for the following reasons:

1. It can mean the difference between successful completion or failure of an investigation.
2. It is stressful to the officer and so must be mastered before it masters the officer's health and well-being.
3. Testimony in one proceeding can be used in another proceeding! Single incidents often are heard in a variety of hearings. A criminal trial's testimony could be used later in a civil proceeding, often to the detriment of the officer.

4. Effective testimony establishes professionalism, while ineffective testimony destroys credibility.
5. The proficiency of testimony can be the determining factor in relationships with local police, clients, etc.

Whatever the setting, the following points are key to being successful:

- Prepare by having all notes and evidence in good order.
- Have proof of corporate existence via a certified copy of the articles of incorporation.
- Be able to establish value of merchandise or extent of damage through a professional assessment. A store buyer, contractor's estimate, etc. should be brought to court.
- Meet with counsel.
- Keep answers short.
- Make eye contact with the trier of fact.
- Be polite, addressing everyone by "sir," "ma'am," or their proper title.
- Avoid absolutes such as "always" and "never."
- Do not guess, speculate, or answer hypothetical questions.
- If unsure about a question, wait for an objection and a ruling on it.

Depositions

Depositions are often engaged in by security personnel in civil proceedings as part of the discovery process. They are usually given at an attorney's office after notices to appear have been sent out to the persons being deposed (deponent). Depositions are formal legal proceedings with court reporters and legal counsel present. Lists of questions are prepared in advance by attorneys and paralegals. Litigation assistants also take notes at the deposition.

While the formal, legal reasons for conducting depositions are to obtain testimony out of court where having such testimony in court is impractical, there are several tactical reasons for depositions:

- Observe and assess the witness.
- Assess the recollection of the opposing witness when they are confronted with unexpected questions.
- Gauge the testimony of the witness and predict what it will be in a subsequent court appearance.
- Obtain testimony in writing for possible impeachment later.
- Identify witnesses known to the witness.
- Require that documents be produced via a request for production.

Being Deposed

- Take the proceeding seriously. Don't be sarcastic or cocky; be very careful that a deposition is taken seriously—even if the setting is relaxed and informal.

Interrogatories

Interrogatories are sets of written questions submitted by one party in a case to the other as part of the discovery process. Interrogatories are usually given under oath, with the person answering them signing a sworn statement that they are true. Interrogatories are submitted to a jury.

Bibliography

R. A. Anderson, I. Fox, and D. P. Twomey (1984). *Business Law*. Cincinnati, OH: South Western.

A. M. Apo (1996). Is it time for premises security standards? *Security Management* 40: 4.

A. Bequai (1990). *Every Manager's Legal Guide to Hiring*. Homewood, IL: Dow-Jones-Irwin.

H. C. Black (1990). *Black's Law Dictionary*. St. Paul, MN: West.
J. Bullock, G. Haddow, D. Coppola, E. Ergin, L. Westerman, and S. Yeletaysi (2006). *Introduction to Homeland Security*. Burlington, MA: Elsevier Butterworth-Heinemann.
D. Cohen (1998). Giving notification where it's due. *Security Management* 42: 3.
R. N. Corley and R. L. Black (1973). *The Legal Environment of Business*. New York, NY: McGraw-Hill.
G. E. Curtis and B. R. McBride (2005). *Proactive Security Administration*. Upper Saddle River, NJ: Pearson Prentice Hall.
C. Garvey (2001). Outsourcing background checks. *HR Magazine* 46: 3.
B. Givens (1997). *The Privacy Rights Handbook: How to Take Control of Your Personal Information*. New York, NY: Avon Books.
J. D. Hartman (1993). *Legal Guidelines for Covert Surveillance Operations in the Private Sector*. Stoneham, MA: Butterworth-Heinemann.
C. A. Hertig (1992). *Civil Liability for Security Personnel*. Bellingham, WA: International Foundation for Protection Officers.
D. J. Horan (1996). *The Retailer's Guide to Loss Prevention and Security*. Boca Raton, FL: CRC Press.
F. E. Inbau, B. J. Farber, and D. W. Arnold (1996). *Protective Security Law*. Newton, MA: Butterworth-Heinemann.
J. C. Klotter (1990). *Criminal Law*. Cincinnati, OH: Anderson.
B. J. Nadell (1998). Timeliness of records now critical. *Security Management* 42: 3.
C. P. Nemeth (1995). *Protective Security and the Law*. Cincinnati, OH: Anderson.
T. K. Schiff (1998). Demystifying worker's comp calculations. *Security Management* 42: 3.
C. T. Thibodeau (1995) Use of Force, Alternatives to the Use of Force, Legal Aspects of the Use of Force. A seminar by Q/A Systems & Consultants, Minneapolis, MN (August).

Legal Aspects of Security

Quiz

1. Reasonable suspicion is more than mere suspicion for it must be based on _____, _____, and _____.

2. Simple negligence is the intentional failure to perform a duty in reckless disregard of the consequences of nonperformance. ☐ T ☐ F

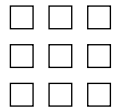
3. Arrest procedures include (select incorrect answer):
   a) Notify the arrestee of the purpose of the arrest.
   b) Be certain to use only reasonable or necessary force.
   c) Restrict searches of arrestees to cursor crushing of the outer clothing for weapons.
   d) Detain arrestee for as long as possible.

4. Children regardless of age can be taken into custody. ☐ T ☐ F

5. Detention may occur for the following reasons (select best answer):
   a) Protect against assault
   b) Stop a trespasser
   c) Conduct an entry or exit search
   d) Recover merchandise
   e) All of the above

6. Should a suit make it to court, what percentage of out of court settlements is given by the defendant?
   a) 10%
   b) 60%
   c) 90%

7. Interrogation under Miranda may only proceed after the suspect makes a "knowing and intelligent waiver" of their rights. ☐ T ☐ F
8. There are various regulations that affect the security industry; most of these are at the _____ and _____, and some are at the _____ and _____.
9. Employers can require employees to give statements regarding disciplinary matters and then use them in criminal prosecution. ☐ T ☐ F
10. Search and seizure by private persons is not normally controlled by the _____.



2 Managing/Supervising to Reduce Liability

Steven R. Ruley

Managing and supervising in the security field is a dynamic and exciting task, which provides the opportunity to make a real difference in the safety and security of others. It is also a difficult and demanding job that requires significant insight and skills to enable you to help those you supervise become effective and productive security officers, investigators, emergency managers, facility managers, and retail loss prevention specialists. Your ability to effectively manage and supervise will not only enhance general safety and security for your employer but will also serve to strengthen the security infrastructure of our nation. These past few years have seen the most dramatic changes in the field of security, with increasing demands, variable resources, and a frequently changing work environment.

Perhaps the most wide-reaching facet of managing and supervising security personnel, and the single issue that can cause the most grief, is that of legal liability; it not only affects relationships with our customers but it also directly affects relationships with our own employees and with the organizations for which we all work.

As a manager and/or supervisor, you are in a unique position due to your responsibilities in helping your organization meet its goals and objectives. Your task of managing and supervising is special, and your work is different from that of most other employees because of the following five principles:

1. Supervising and managing are *fundamentally* different from other types of general work.
2. Supervisors and managers are generally responsible for planning, organizing, directing, staffing, and controlling the work of others.
3. You play a key role in applying skills to meet the needs of your organization because you represent the entire organization in your role as a supervisor/manager.
4. Your performance will be judged, in part, by the results you and those you supervise and manage are able to obtain with the resources you are given.
5. Your actions will be guided by the dynamics of each situation, and your ability to interpret and apply rules and regulations.

You will have three basic roles as a security supervisor or manager. Each of the following roles is critical to your ability to reduce liability:

1. Interpersonal role: This is where your ability to inspire and lead other people comes to the forefront. As a supervisor, you will be working directly with employees. It is in this role that you have a tremendous opportunity to project honesty, integrity, and the type of attitude that is critical to the overall success of a security function. Honesty, integrity, and proper attitude are core values for security supervisors, managers, investigators, emergency managers, facility managers, and loss prevention specialists, and a deficiency in any of these areas is the first step toward major liability issues. This is also where you will be dealing with employees on an individual basis, and where you must ensure that

your employees are treated in accordance with the laws that are designed to guarantee fairness and safety in the working environment. This role will also expose you to the intricacies of selecting and hiring security employees. This is another area of potential liability where you can play a key role in managing risk and reducing liability.

2. Informational role: In this role, you are expected to be a fountain of legally correct information, and to disseminate that information to each of your employees so that they clearly understand their jobs, what is expected of them, and what they legally can and cannot do in the context of their employment. In your informational role, you are responsible for *training*. Most employees, if they have been properly screened and selected, actually want to do a good job and are eager to learn. Your role is to provide them with the best information and the most current information available to enable them to perform their duties in an efficient and legal manner. Employees that are adequately trained will have the necessary tools to do the job, will be better motivated and more confident, and will reduce your liability exposure.
3. Decisional role: This final role is what people often think about when considering the responsibilities of supervisors and managers. Your decisional role is a form of crisis management; you will be the leader who must decide how best to handle unusual situations. This role will place you into the position of making decisions that will directly affect the customers of your organization, the public, and often, your own employees. These decisions may range from basic things such as who is working on what shift or how many people will be assigned to work a particular event or detail to complex decisions relating to arrests, detentions, and other actions that may directly impact the civil and legal rights of others.

Each of these three basic roles in which you will serve as a supervisor or manager presents various challenges and problems. You will need three types of *skills* to successfully handle these roles and reduce the unnecessary exposure of liability to your employees, your boss, your customers, and yourself. These basic skills apply equally to all supervisors and managers, as well as to investigators, emergency managers, Homeland Security personnel facility managers, and loss prevention specialists, and include the following:

1. Conceptual skills: These are basic managerial skills that give you the ability to analyze situations, interpret laws, rules and regulations, and to solve problems in a reasonably effective manner. If you have poor conceptual skills, you will be inclined to misinterpret situations and to apply incorrect or improper methods of handling problems. This can quickly lead to an unnecessary liability exposure. Conversely, solid conceptual skills will enable you to quickly recognize and avoid problem areas and to provide sound decisions that reflect good risk management techniques.
2. Human relation skills: These are arguably the most important of the skills you need to effectively manage and supervise. They are especially important because they enable you to interact with the public and with those you supervise and manage in a way that is both effective and efficient. I used to think that the old adage "You can catch more flies with honey than with vinegar" was great, if your objective was to catch flies. However, in the security supervision and management arena, it is a good analogy. The majority of the problems you will face can be resolved if you are straightforward and personable. Good human relation skills are displayed in your ability to be pleasant with people whenever possible, to be firm when necessary, and to be fair at all times. Managers and supervisors with good human relation skills have employees and customers who genuinely respect them and can communicate freely. Communication is another key element in avoiding unnecessary liability situations. *It has often been said that the majority of civil lawsuits results from a simple (and avoidable) lack of effective communication*. To summarize, human relation skills are extremely important because they better enable you to avoid problems in the first place and to negotiate through problems that are sometimes unavoidable. For these reasons alone, good human relation skills are often able to make up for minor deficits in other skill areas.

3. Technical skills: These are the basic skills you possess that allow you to operate in the security environment. They include your basic training and management training, and relate directly to the technical aspects of your job and the jobs of each of those that you supervise and/or manage.

Liability: What Is It?

Black's Law Dictionary defines liability as a "broad legal term which has been referred to as of the most comprehensive significance, including almost every character of hazard or responsibility, absolute, contingent or likely." In simpler terms, liability is a legal concept under which a person (*you*) may be held responsible by another person, and required to make good on any losses or damages you may have caused. It is a simple concept that has become extremely complex due to a large body of conflicting legal decisions. When you couple that with a society that often seems driven to sue anybody for anything, you can easily see why any efforts to reduce liability are worthwhile.

Liability is a *risk* just like other risks, which we face every day. Because it is a risk, it can be *managed* by the application of *risk management techniques*. These techniques include the following:

1. Recognition: It is important to recognize the various types of liability exposure.
2. Education: Liability can be reduced and minimized if both management and employees are thoroughly trained in *all* of the aspects of their jobs and in liability avoidance techniques.
3. Supervision: The best educational programs will not be effective in reducing liability if they are not accompanied by effective supervision.
4. Documentation: Report writing and documentation of facts are a basic part of security work. Yet, when it comes to incidents where we are exposed to potential liability, there is often an amazing lack of documentation. We must document *all* of our activities in order to reduce our liability exposure. This includes security incidents, training, and counseling we provide to those we supervise and manage, complaints we receive, and evaluations we make concerning our employees. Each of these records must thoroughly and honestly document the facts because someday they may be important in the defense of a liability case.

Liability exists in *two basic forms*:

1. Civil liability, in which you may be subjected to a lawsuit for your actions (or for your failure to act, where necessary) and
2. Criminal liability, in which you may be subjected to potential criminal charges for acts performed (or not performed where required).

Just to make things more interesting, remember that it is also possible to face *both* civil and criminal liabilities at the same time!!

Civil Liability

Civil liability is presented when an act, known as a *tort*, is committed against another. In the security field, including investigations, Homeland Security, facility management, loss prevention, etc., we are generally concerned most frequently with the following torts:

1. Intentional torts: These are torts in which an act occurs and you *could have* or *should have* known that it would likely cause damages. To prove an intentional tort, you must have the following:
   (a) The act
   (b) Intention of consequences
   (c) Causation (what you did or did not do caused the result)
   (d) Damages

The intentional torts are generally defined as assault, battery, conversion, false imprisonment, intentional infliction of emotional distress, trespass to land, and trespass to chattels.

Intentional torts can be committed against *persons*. Examples of torts against persons would include:

1. Battery: A harmful or offensive contact, judged by a "reasonable person" standard. No actual damages are required.
2. Assault: Deliberately placing a person in fear of an immediate battery. (The apparent ability to cause harm is insufficient. An overt act is required. Words coupled with conduct.) No proof of actual harm is required.
3. False imprisonment: An act or omission that results in the confinement of a person to a bounded area, coupled with awareness by the person that they are, in fact, confined. The length of time confined is immaterial.
4. Intentional infliction of emotional distress: This is a frequent tort seen in the security field. This tort requires an act of *extreme* and *outrageous* conduct toward someone of known sensitivity. Good examples include children, pregnant women, sick people, the elderly, etc. Actual damages are required and would include evidence of physical harm resulting from the extreme and outrageous act.

Intentional torts can also be committed against *property*. Examples include:

(a) Trespass to land: This requires a physical invasion of the land. Under common law (traditional case law) no proof of actual damages is required, that is, if you step on someone else's land and cause no damage, you have still committed a trespass. The person committing the tort is liable for all consequences.
(b) Trespass to chattel: An act that interferes with a person's right to possession of property (other than land). This is a tort occasionally seen in the security work when a person is wrongfully restricted from entering or using his or her property.

There are several defenses that may be used to defend against intentional torts. These include the following:

(a) Consent: Consent may be given voluntarily. It is important to remember that a person giving consent must be legally capable of giving it, that is, the person cannot be mentally incompetent, intoxicated, senile, a young child, etc. Consent must not be induced by *fraud*.
(b) Self-defense: You must have a reasonable belief as to the necessity of the act, that is, you had to do what you did to defend yourself from death or serious injury.
(c) Defense of others: You may argue that you acted to defend another. Generally speaking, you may defend others from death or serious injury with the same level of force you could legally use to defend yourself.
(d) Defense of property: This is limited to the preventing of the commission of a tort. *The use of* deadly force is not allowed *in the defense of property*.
(e) Necessity: You may defend an intentional tort if the threatened injury you prevent is substantially more serious than the actions you take to prevent it. As an example, if you physically take a telephone from someone in a phone booth for the purpose of calling for help to save someone's life, you may use *necessity* as a defense.

Probably the greatest single area of concern in civil liability to the security supervisor or manager is that of *negligence*. A significant portion of liability exposure to you, your employees, and your company will come in this area of the law.

In order to prove a case of *negligence*, four elements must be proven by the Plaintiff. These four elements include the following:

1. Duty: (usually a duty to protect against unreasonable risk of injury). This duty is normally that of a reasonable, ordinary, and prudent person. However, professionals (such as security supervisors/managers) have a *higher degree of duty*, and must act with the same level of skill, knowledge, and care, as would a practitioner in

a similar setting in the community. This simply means that security professionals are expected to act with the same degree of skill as is generally accepted in the profession.

2. Breach of duty: To prove a breach of duty, you must show the facts of an occurrence *and* show that the action taken was unreasonable under the applicable standard of care. Along with this, proof needs to be shown that the injury would not have happened without negligence and that what caused the injury was within the exclusive control of the defendant.
3. Causation: This means that the act was either the cause in fact *or* the proximate cause of the injury, that is, the injury would not have happened "but for" the breach of duty, which resulted in the negligence.
4. Damages: This is an actual injury or loss that happened because of the negligence. Injured parties have a duty to mitigate or minimize their damages. If negligence results in personal injury, the victim is entitled to compensation for all damages. If negligence results in property loss or damage, the victim is entitled to *reasonable* cost of repair *or* the *fair market value*. In some cases, *punitive damages* may be available, particularly if the acts done were intentional and malicious.

There are also several defenses to the tort of negligence. These include:

(a) Contributory negligence: This means that the victim was also negligent, and because of that, "contributed" to the cause of the damages.
(b) Comparative negligence: This defense assigns various percentages of negligence to each party and allows recovery in a ration to fault.
(c) Assumption of risk: This theory states that the victim either expressed or implied voluntary assumption of the known risk.

As you can see, there are many instances in security work where negligence can be claimed. This can include negligent hiring of personnel, negligent retention of unsuitable employees who should have been terminated, negligent training, and negligent supervision. All of these areas of negligence impact on *you*, the supervisor or manager.

And, speaking of you, these are lawsuits in which you do not want to find yourself on the receiving end:

- Negligent hiring: The hiring of people that are unsuited for this type of work and responsibility. Not conducting appropriate psychological examinations, or not conducting full background checks. It is awkward, at best, trying to explain why you hired a convicted felon and placed them in a position providing direct access to large sums of money.
- Negligent supervision: The inadequate monitoring of employee performance. Failing to reprimand when appropriate; failing to check out complaints against your subordinates, generally not doing your job.
- Negligent retention: Keeping employees on the job when it is clear they should be terminated. Promoting employees based on favoritism or friendship in the face of facts that they should have been demoted, or dismissed, or at least disciplined.
- Failure to protect: Not providing the required protection when an expectation of protection has been established. If you make it known that there are security cameras and they are monitored, and someone gets injured or experiences a loss because they were not monitored, watch out for this one.
- Failure to direct: Not giving your subordinates clear and concise guidance on how to perform their duties. Failing to have policies and procedures, or failing to follow those policies and procedures so that they are essentially meaningless.
- Failure to train: This speaks for itself. If you do not adequately prepare your employees to do their job, and someone experiences damages because of it, prepare to drain your bank account.
- Negligent assignment: Assigning an employee with a known problem to a critical and improper position.

- Failure to investigate: If and when you receive complaints about employees, or about the facility you are securing or managing, you have a basic and fundamental duty to investigate and resolve the problem. Failure to do so is evidence if negligence.
- Failure to discipline: Not establishing and utilizing a formal process for discipline.

As you can see, there are lots of things you, as a supervisor or manager, can fail to do, and for which you can be held liable, civilly and/or criminally. But the good news is that most of these can be avoided with the use of common sense, dedication to duty, and an effective working relationship with your organization's legal advisor.

Other General Areas of Liability

Now that you have been briefly introduced to the intentional torts and negligence, you should also be aware of a few more areas in which the security industry is particularly vulnerable to liability. These areas include the following:

1. Nuisance, which is defined as either being private or being public.
   A private nuisance is the substantial, unreasonable interference with another person's use or enjoyment of their property (land).
   A public nuisance is the unreasonable interference with the health, safety, or property rights of the *community*.
   Legal remedies for nuisance can involve payment of money damages to the victim(s) and/or Injunctive Relief in which the court issues an order to stop doing whatever it is you were doing that was a nuisance.
2. Defamation: This is a very sensitive area for liability in the security industry. It is most often seen when an improper arrest has been made and the arrestee has lost status as a result of the improper arrest. It is occasionally seen in investigative cases in which information is improperly disseminated and the victim loses status or reputation or is otherwise damaged by leaked information that should have remained confidential. Defamation is subdivided into two general categories:
   (a) Libel, which requires the publication of defamatory information about the Plaintiff, that is, it is put into writing and disseminated to others, and
   (b) Slander, which is the spoken word that includes defamatory information about the victim.
   (c) There are different standards of proof required to prove defamation between a "public figure" and a private citizen. Generally speaking, public figures are subject to more public scrutiny, and it is more difficult to prove defamation concerning a public figure.

   Defenses to defamation include:

- Consent (the victim consented to your actions);
- Truth of statement (if you are telling the truth, you cannot be defaming the person);
- Absolute privilege (which occurs in judicial, legislative, and executive proceedings);
- If you were forced into your actions against your will;
- Communications between *spouses*; and
- Qualified privilege (such as public reporting, or the special interest of the recipient such as your client).

Another area of special interest to the security field is that of *invasion of privacy*. There are several actions that would constitute this tort, but, from a security standpoint, it is most often an act of prying or intruding into another person's private affairs that would be objectionable to a reasonable person. Also, publication of information, which portrays the victim in a "false light," and the public disclosure of private facts that a reasonable person with ordinary sensibilities would find objectionable could also constitute this tort. If you do any of these things and actually cause damages (emotional distress is sufficient), you are liable for this action. As with the tort of defamation, this tort can be defended if you had *consent* to perform your actions by the victim or if you had a *privilege* to perform your actions.

It is important for you to recognize that all of these civil liabilities will affect not only your employees but also may very well affect you and your organization. Because of a legal doctrine known as *vicarious liability*, you and your company may be held liable for the actions of your employees. This is defined even further under the doctrine of *respondeat superior*, which clearly makes employers (supervisors and managers) liable for torts committed by their employees *if the employee was acting within the scope of his or her employment*.

This doctrine of respondeat superior is the legal theory under which employers may be held liable for the intentional acts of their employees, and is where you can be held liable for such things as negligent hiring, negligent supervision, negligent entrustment, negligent retention of the employee, and negligent selection of the employee.

Employment Liability

In addition to the general areas of civil liability that can involve you and those you supervise and manage, you are also exposed to liability in your actions relating to how you treat your employees, and the laws that surround this area of function.

For the past several years, employment laws have been changing, and case law has been developing in order to guarantee certain rights and privileges to employees. As a manager and/or supervisor, your employees are your most valuable assets, and it is beneficial to have those protective laws in place. However, you must also recognize that each of these laws, rules, and regulations will restrict you in the manner in which you staff and supervise your operation.

The laws governing employees may be categorized into three general areas:

1. Assurance of equal employment opportunities.
   These laws guarantee the right to be employed and to advance in employment based on merit, ability, and potential without discrimination because of race, color, religion, sex, age, or national origin. The *Equal Employment Opportunity Commission* (EEOC) enforces these laws.
2. Assurance of safe and healthful working conditions.
   These laws guarantee employees' safety on the job by requiring provision of safety equipment where needed, by requiring training on safety matters, and by requiring that employees be made aware of hazards in the workplace and how they are to be handled. Most of these laws were implemented under the Occupational Safety and Health Act of 1970 (OSHA) and are enforced by either federal or state occupational safety agencies.
3. Assurance of fair compensation and collective bargaining.
   These laws concern minimum wages and working conditions, and also cover general labor relationships between workers and management. The National Labor Relations Board (NLRB) enforces collective bargaining issues.

Each state has its own set of labor and employment laws, and you should make every effort to be at least generally familiar with them and their provisions.

You should also be acquainted with the major federal laws concerning equal employment. These include:

Equal Pay Act of 1963: Provides for equal pay for equal work between men and women.

Title VII of the Civil Rights Act: Prohibits discrimination.

Age Discrimination in Employment Act: This was amended in 1978 to protect workers between the ages of 40 and 70 from being forced into retirement or other positions.

Pregnancy Discrimination Act of 1978: Protects pregnant women from job discrimination.

Americans with Disabilities Act of 1991: Prohibits discrimination based on disabilities.

All of these laws are voluminous and beyond the scope of this chapter. However, each of them is important and can result in liability to you or your organization if they are not properly observed and enforced. Time spent learning about the laws under which you must work is time well invested and will be very helpful to you in reducing your exposure to liability.

One final area of employment law that is receiving a great deal of attention in both the courts and the media is that of *sexual harassment*. This is a form of gender discrimination

that violates Title VII of the 1964 Civil Rights Act and also violates the discrimination laws of most states.

In the employment setting, there are two types of sexual harassment:

1. Quid pro quo: where employment decisions (hiring, firing, promotions, assignments, etc.) are based on an employee's willingness to grant or deny sexual favors.
2. Hostile environment: where verbal and/or nonverbal behavior on the job is sexual or gender based in nature, is unwanted or unwelcome, and is severe or pervasive enough to affect the victim's work environment. Hostile work environment complaints now extend well beyond those based only on sexual harassment, and now includes employees that are generally hostile and offensive to others on a continual basis.

Suffice it to say that the cost of defending one of these lawsuits is tremendous, not to mention the costs in terms of public relations, lost business, and employee morale. With proper training, good attitudes, and prevention, these lawsuits may be avoided entirely.

Prevention of sexual harassment charges requires you or your organization to prepare and distribute (and train on) a clear and concise policy prohibiting gender harassment. As a supervisor, you need to make certain that this policy is well publicized and discussed among your employees. You should provide in-house training and awareness seminars, and you should develop a complaint procedure.

If you are unfortunate enough to have one of these complaints presented to you, the complaint should be evaluated and investigated without undue delay. The investigation should be documented. If the complaint is valid, appropriate corrective action should be taken immediately.

This is a very sensitive issue that requires all of your abilities as a supervisor to reassure the complainant; to insure a fair, thorough, and impartial investigation; and to communicate to all involved parties what is being done.

Criminal Liability

Besides the civil liabilities we have already discussed, security personnel are also subject to criminal liability, just like any other citizen, if they violate the law.

The criminal areas most frequently affecting security employees include the following:

- Trespass
- Harassment
- Entrapment (if you are working with law enforcement)
- Conspiracy
- Impersonating
- Reckless endangerment
- Obstructing public rights of way

In addition to this limited list, there are as many potential criminal liabilities as there are criminal laws. You can avoid unnecessary criminal liability for your organization by proper screening of personnel, by conducting regular training of your personnel, and by doing your job in providing adequate supervision to prevent and correct problems while they are still minor.

Often security work, and investigative work, involves situations where your personnel will be performing duties that are very similar to those of public law enforcement. It is absolutely imperative that staff understands the differences between public law enforcement and private security, so that your staff does not perform any functions or exercise any privileges, which are not authorized by law. The public is often confused about the differences between public and private enforcement agents, and this is an area where liability lurks.

What does it All Mean?

Now that you have had a brief introduction to some of the things that can go wrong and result in legal liability, you may be asking yourself if it would be safer to just quit your job,

lock yourself up in a dark room, and wait quietly until your time on this planet is over! With all of the problems out there, is it really worth it?

Of Course It Is!!!

The security profession, including supervisors and managers, investigators, facility managers, homeland security professionals, and loss prevention specialists (to name just a few), is a critically important part of our society. We are the eyes and ears and the very first line of defense for our employers and their customers. We protect and we serve, just as doctors, paramedics, lawyers, police officers, and firefighters do.

All of this liability business sounds serious, and it should. It is serious. But by reading and understanding this introduction, you have taken that first critical step to reduce your risks and your liability.

If you prepare yourself as a supervisor and as a manager, and do your job as it should be done, you have already won more than half of the battle. As a supervisor/manager, you have both a personal and a professional interest in selecting the best people to work in our industry, training these people as often and as well as you can with the resources available to you, in promoting their development as security officers, and in providing strong, fair, and effective supervision.

Remember: you are the key to reducing liability in our chosen profession

Bibliography for Further Reading

R. L. Bintliff (1992). *The Complete Manual of Corporate and Industrial Security*. Prentice-Hall.

L. R. Bittel (1989). *The McGraw Hill 36 Hour Management Course*. McGraw-Hill Publishing Co.

R. D. Blanchard (1990). *Litigation and Trial Practice for the Legal Professional*. West Publishing Company.

G. E. Dix (2000). *Criminal Law, Gilbert Law Summaries*, 16th edn. Harcourt Professional Education Group, Inc.

L. J. Fennelly (1989). *Handbook of Loss Prevention and Crime Prevention*. Butterworth-Heineman.

J. D. Hartman (1993). *Legal Guidelines for Covert Surveillance in the Private Sector*. Butterworth-Heineman.

F. Inbau, M. E. Aspen, and J. E. Spiotto (1993). *Protective Security Law*. Butterworth-Heineman.

W. P. Keeton, D. B. Dobbs, R. E. Keeton, and D. G. Owen (1984). *Prosser and Keeton on Torts*, 5th edn. West Publishing Company.

W. P. Statsky (1982). *Torts: Personal Injury Litigation*. West Publishing Company.

Managing/Supervising to Reduce Liability Quiz

1. Supervisors and managers are generally responsible for planning, _____, and directing.
2. In order to provide a case of _____, four elements must be present.
3. Slander is the spoken word including _____ information about the victim.
4. Assurance of _____ and healthful working conditions.
5. Besides the _____ liability, security personnel are also subject to criminal liability.
6. The two basic forms of liability are *civil liability* and *criminal liability*. ☐ T ☐ F

7. Assumption of risk is one defense to the *tort of negligence*. ☐ T ☐ F
8. The substan tial, unreasonable interference with another person's use or enjoyment of property is a *public nu*isance. ☐ T ☐ F
9. Libel is the spoken word, including defamatory information about the victim. ☐ T ☐ F

3 Sexual Harassment

Brion P. Gilbride

In recent years, sexual harassment in the workplace has become more and more evident, just as more focused efforts have been made to prevent it. As a security manager one can expect to be called on to deal with this type of behavior, especially in larger companies where many employees are female. In order to cope with sexual harassment, the security manager must be aware of what it is as well as what remedies may be used to correct it.

Most people are aware of sexual harassment now that case law has brought the issue into public discourse. Statistics as of 1997 indicate that the increased awareness of sexual harassment is changing things. Some of these changes are beneficial and some are not. Anita Hill, in an editorial in the *New York Times* stated that "Last year, more than 17,000 sexual harassment claims were filed with the EEOC."[1] An article on insurance for sexual harassment indicated another statistic. "Federal reports of sexual harassment have more than doubled, from 6,883 in 1991 to 15,889 in 1997."[2] The judgments in these cases that are decided in favor of the victim are also interesting. "A jury awarded $80.7 million to a former UPS employee for accusing a coworker of poking her in the breast," and from 1991 to 1997 "monetary awards in federal sexual harassment suits rose from $7.1 million to $49.4 million."[3] In a court case decided in February 1998, "Astra USA, Inc., a pharmaceutical company in Westboro, MA, agreed to pay $9.85 million in a sexual harassment settlement."[4]

Statutory Definitions

Title VII

The legal basis of all the complaints, litigation, decisions, and laws regarding the many facets of sexual harassment stem from Title VII of the Civil Rights Act of 1964. Although legally known as Title 42 of the United States Code (USC), Section 2000(e), it is commonly referred to as Title VII. This law establishes basically an employer cannot discriminate against a U.S. citizen or U.S. citizens because of their gender.

In its simplest form, Title VII's essence can be found in Title 42, USC, Section 2000(e)(2)(a), which states that:

> *It shall be an unlawful employment practice for an employer— 1) to fail or refuse to hire or to discharge any individual, or otherwise to discriminate against any individual with respect to his compensation, terms, conditions,*

---

1 Anita Hill (March 19, 1998). A matter of definition. *New York Times*, p. A25.

2 (March 23, 1998). Insurers issuing more policies to help handle harassment. *The York Daily Record,* p. 3A.

3 Shaheena Ahmad (March 2, 1998). Get your sex insurance now. *US News and World Report,* p. 61.

4 Insurers issuing more policies to help handle harassment, p. 3A.

> *or privileges of employment, because of such individual's race, color, religion, sex, or national origin; or 2) to limit, segregate, or classify his employees or applicants for employment in any way which would deprive or tend to deprive any individual of employment opportunities or otherwise adversely affect his status as an employee, because of such individual's race, color, religion, sex, or national origin.*[5]

This definition is somewhat "wordy," as most laws are, but it says an employer cannot fire or refuse to hire a person because of their sex. It also says an employer cannot engage in any organization of its workplace or job applicants in such a way that it might cause a person to be discriminated against because of their sex.

The architects of the Civil Rights Act of 1964 also added a section to Title VII that states that an employment agency cannot refer or refuse to refer a person for employment or otherwise discriminate against them because of or on the basis of their sex. If an employer utilizes contract employees or has an employment agency office on-site, this section may be applicable as well.[6]

Another section of Title VII that could affect an employer regards labor organizations or unions. It states that a labor union cannot exclude or expel any person from membership because of his or her sex. It further states that a union cannot engage in any organization of its membership or applicants for membership in such a way that an individual might be discriminated against on the basis of sex.[7] In many unions, particularly in companies large enough to have their own Union chapter, union management officers may also be employees of the company. This is particularly true of government employment at the Federal level.

Title VII does make one interesting exemption to its prohibition of discrimination based on sex:

> *g)…it shall not be an unlawful employment practice for an employer to fail or refuse to hire and employ any individual for any position, for an employer to discharge any individual from any position, or for an employment agency to fail or refuse to refer any individual for employment in any position, or for a labor organization to fail refuse to refer any individual for employment for any position, if—the occupancy of such position, or access to the premises in or upon which any part of the duties of such a position is performed or is to be performed, is subject to any requirement imposed in the interest of the national security of the United States under any security program in effect pursuant to or administered under any statute of the United States or any Executive order of the President; and such individual has not fulfilled or ceased to fulfill that requirement.*[8]

Even though this law was passed at the height of the Cold War, it is interesting that an exemption was made for matters of national security when this law was passed 37 years prior to the attacks of September 11, 2001.

Title VII also had the effect of creating the Equal Employment Opportunity Commission (EEOC), which at its inception was authorized to have five members, "not more than three of whom shall be of the same political party." The members of this commission are appointed by the sitting president of the United States for a five-year term, with the consent of the U.S. Senate.[9] Later on, we will discuss the EEOC, its operations, and decisions the EEOC has made that affect sexual harassment law and commentary.

---

[5] 42 USC 2000(e)(2)(a).
[6] 42 USC 2000(e)(2)(b).
[7] 42 USC 2000(e)(2)(c).
[8] 42 USC 2000(e)(2)(g).
[9] 42 USC 2000(e)(4)(a).

There are definitions in Title VII for some of the terms used within the Title that should be mentioned here. These definitions, by their presentation, do somewhat change the meaning of Title VII.

> *Person: one or more individuals, governments, governmental agencies, political subdivisions, labor unions, partnerships, associations, corporations, legal representatives, mutual companies, joint-stock companies, trusts, unincorporated organizations, trustees, trustees in cases under title 11 (bankruptcy), or receivers.*[10]

To some, that would seem like a thorough definition. It *is* a thorough definition, unlike "employee," which has some exemptions attached to it.

> *Employee: an individual employed by an employer, except that the term "employee" shall not include any person elected to public office in any State or political subdivision of any State by the qualified voters thereof, or any person chosen by such officer to be on such officer's personal staff, or an appointee on the policy-making level or an immediate adviser with respect to the exercise of the constitutional or legal powers of the office.*[11]

In short, this means that any elected official *and* anyone on their staffs or appointed by that official is not considered an "employee." In case the definition of "employee" was not confusing enough, an exemption to the statement regarding elected officials states: "The exemption set forth in the preceding sentence shall not include employees subject to the civil service laws of a State government, governmental agency or political subdivision."[12]

In a time when many companies as well as government and quasi-government agencies have some type of proprietary or contract security on their premises, this exemption could also have implications.

Title IX

After Title VII was enacted, it was concluded that Title VII protection did not extend to colleges, universities, and other postsecondary educational institutions. These protections were added into Title IX of the Education Amendments of 1972. Although legally referred to as Title 20, Sections 1681–1688 of the USC, this collection of laws is called "Title IX."

Title IX says that no one can be excluded from, denied participation in, or otherwise discriminated against in any educational program or activity that receives financial assistance from the Federal government. It also specifically states that Title IX applies to the admissions process:

> *…in regard to admissions to educational institutions, this section shall apply only to institutions of vocational education, professional education, and graduate higher education, and to public institutions of undergraduate higher education.*[13]

Like its counterpart, Title IX also is chock-full of exemptions to the rules. Religious schools are exempt from Title IX if "application…would not be consistent with the religious tenets of such organization." Military and merchant marine academies are also exempted. Social fraternities and sororities, which are found in many higher education institutions, are exempt from Title IX protections.[14]

---

10 42 USC 2000(e)(a).
11 42 USC 2000(e)(f).
12 42 USC 2000(e)(f).
13 20 USC 1681(a)(1).
14 20 USC 1681(a)(3–6).

On a more interesting note: Title IX does say that if an institution "traditionally and continually from its establishment" has had a policy of admitting students of one sex, it is also an exemption.[15] It also says that the Young Men's Christian Association (YMCA), the Young Women's Christian Association (YWCA), the Girl Scouts of America, and the Boy Scouts of America are also exempted from Title IX protection.[16]

There are many stories in the news these days about colleges and universities having to alter or eliminate sports programs for men in order to accommodate Title IX requirements for women's sports programs. What was lost in the shuffle during public debate on the issue was the following portion of Title IX:

> *Nothing contained in subsection (a) of this section shall be interpreted to require any educational institution to grant preferential or disparate treatment to the members of one sex on account of an imbalance which may exist with respect to the total number of percentage of persons of that sex participating in or receiving the benefits of any federally supported program or activity, in comparison with the total number or percentage of persons of that sex in any community, State, section, or other area: provided that this subsection shall not be construed to prevent the consideration in any hearing or proceeding under this chapter of statistical evidence tending to show that such an imbalance exists with respect to the participation in, or receipt of benefits of, any such program or activity by members of one sex.*[17]

This is certainly open to debate, but it appears to say that an institution is *not* required to change its programs in order to have a more proportionate balance of male versus female programs and activities. What it also says is that institutions are *not prohibited* from making an argument that such balance should exist and that institutions *may consider* statistical evidence that supports changing their programs in such a fashion during legal proceedings initiated in accordance with Title IX. The Commission on Opportunity in Athletics, which was due to report its findings on Title IX in January, 2003, is examining this "proportionality" issue and indications are that the Commission is aware of the misinterpretation of statements made in Title IX mentioned above.[18]

In the 21st century, many colleges and universities are coeducational or "coed," meaning that they admit students of either sex. Many of these institutions maintain either living quarters on-campus or support residences for the students off-campus. These living quarters, until recently, have been segregated by sex. Title IX specifically states that housing units maintained separately for each sex is permissible.[19]

Title IX, like its counterpart Title VII, has definitions contained within that might influence interpretation of the law.

> *Program or Activity: For the purposes of this title, the term "program or activity" and "program" mean all of the operations of:*
>
> *1a) a department, agency, special purpose district, or other instrumentality of a State or local government; or*
> *1b) the entity of such State or local government that distributed such assistance and each such department or agency (and each other State or local government entity) to which the assistance is extended, in the case of assistance to a State or local government;*
> *2a) a college, university, or other postsecondary institution, or a public system of higher education; or*

---

15 20 USC 1681(a)(5).
16 20 USC 168 1(a)(6)(B).
17 20 USC 1681(a)(9)(B).
18 Mark Alesia (December 20, 2002). Danger seen for Title IX. *Indianapolis Star*.
19 20 USC 1686.

2b) a local educational agency…system of vocational education, or other school system

3a) an entire corporation, partnership, or other private organization, or an entire sole proprietorship if assistance is extended to such corporation, partnership, private organization, or sole proprietorship as a whole; or

which is principally engaged in the business of providing education, health care, housing, social services, or parks and recreation; or

3b) the entire plant or other comparable, geographically separate facility to which Federal financial assistance is extended, in the case of any other corporation, partnership, private organization, or sole proprietorship; or

4) any other entity which is established by two or more of the entities established in paragraphs 1, 2, or 3; any part of which is extended Federal financial assistance, except that such term does not include any operation of an entity which is controlled by a religious organization if the application of section 1681 of this title to such operation would not be consistent with the religious tenets of such organization.[20]

That was quite lengthy, unfortunately, but it covers essentially any entity engaged in education, health care, parks and recreation, housing, or social services, and it includes entities from both the private and public sectors. It only exempts organizations with religious affiliation.

Having covered the major Federal law regarding sexual harassment and discrimination based on sex, State law regarding these topics must also be examined. To include all 50 U.S. states would be prohibitive; the following is merely a sample.

Massachusetts, for example, has Title 21, Chapter 151-B of the General Laws of Massachusetts. It prohibits "unlawful discrimination because of race, color, religious creed, national origin, ancestry or sex."[21] This law contains sections for establishing a harassment policy and training programs, and even states how often a company must transmit its harassment policy to employees. Further, Title 21, Chapter 151-B, Section 4, which identifies unlawful employment practices, is written similarly to Title VII. It also includes the following statements:

3A. For *any person engaged in the insurance or bonding business, or his agent, to make any inquiry or record of any person seeking a bond or surety bond conditioned upon faithful performance of his duties or to use any form of application in connection with the furnishing of such bond, which seeks information relative to the… sex…or ancestry of the person to be bonded.*

3B. For any person whose business includes granting mortgage loans or engaging in residential real estate-related transactions to discriminate against any person in the granting of any mortgage loan or in making available such a transaction, or in the terms or conditions of such a loan or transaction, because of… sex… Such transactions shall include, but not be limited to:

(1) the making or purchasing of loans or the provision of other financial assistance for purchasing, constructing, improving, repairing, or maintaining a dwelling; or the making or purchasing of loans or the provision of other financial assistance secured by residential real estate; or

(2) the selling, brokering, or appraising of residential real estate.[22]

Title X of the New Jersey Permanent Statutes covers Civil Rights. Like the Massachusetts statute, it contains some items of interest that go above and beyond the scope of Title VII.

---

[20] 20 USC 1687.

[21] Title 21, Chapter 151(B), Section 3A of the General Laws of Massachusetts.

[22] Title 21, Chapter 151(B), Section 4 of the Massachusetts General Laws.

Title X contains sections that establish penalties for violating New Jersey's prohibition against discrimination and for providing attorneys fees to the winner of a discrimination claim. New Jersey also classifies these items as criminal laws; violations of some sections of Title X are classified as a misdemeanor offense. They read:

> *10:1-6. Penalty and punishment*
>
> *Any person who shall violate any of the provisions of sections 10:1-2 to 10:1-5 of this Title by denying to any citizen, except for reasons applicable alike to all citizens of every race, creed, color, national origin, ancestry, marital status or sex and regardless of race, creed, color, national origin, ancestry, marital status or sex, the full enjoyment of any of the accommodations, advantages, facilities or privileges in said sections enumerated, or by aiding or inciting such denial, or who shall aid or incite the violation of any of the said provisions shall, for each and every violation thereof, forfeit and pay the sum of not less than $100.00 nor more than $500.00, to the State, to be recovered in a civil action, with costs, and shall also, for every such violation, be deemed guilty of a misdemeanor, and upon conviction thereof, shall be subject to a fine of not more than $500.00, or by imprisonment of not more than 90 days, or both.*[23]
>
> *10:1-7. Jurisdiction; costs and attorney's fees*
>
> *The aggrieved party or parties in any action authorized by R.S.10:1-6 may institute said action in the name of the State of New Jersey in the Superior Court. If judgment is awarded in favor of the plaintiff in such action, the aggrieved party shall be paid out of the judgment so recovered, the costs incurred in prosecuting such action, according to a bill of costs to be taxed as hereinafter provided, and also an attorney's fee of not less than twenty dollars ($20.00) nor more than one hundred dollars ($100.00) to be determined and fixed as hereinafter provided.*
>
> *The bill of costs shall be taxed by the clerk of the court as in other civil actions within the jurisdiction of the court. The amount of the attorney's fee shall be determined and fixed by an order of the court.*[24]

Thus far, the Federal statutory background for sexual harassment complaint has been covered in this chapter. In addition, two State statutes are also covered for comparison. It is common for State law to mimic and then expand on Federal law, and the Massachusetts and New Jersey laws are fine examples of that principle.

Development of Harassment Case Law 1970–2001

Case law as it relates to harassment actions developed because of racial discrimination claims that began appearing after the Civil Rights Act of 1964 was passed. The courts' handling of these claims eventually produced a landmark case, *Meritor Savings Bank v. Vinson*, which was decided by the U.S. Supreme Court in 1986. Recent cases, such as *Faragher v. City of Boca Raton*, have further defined what constitutes a sexual harassment claim as well as defenses that may or may not be used by an employer. *Faragher* was decided in 1997.

The 1970s

The precursors to sexual harassment case law began appearing in 1971. *Griggs v. Duke Power Co.* was heard by the Supreme Court. The Court held that the Civil Rights Act of 1964 required the elimination of "artificial, arbitrary, and unnecessary barriers" that discriminate based on race. Furthermore, the Court prohibited any employment practice that can be considered discriminatory unless it can be shown to be related to job

---

[23] Title 10, Section 1-6 of the New Jersey Permanent Statutes.

[24] Title 10, Section 1-7 of the New Jersey Permanent Statutes.

performance.[25] In a somewhat interesting side note, the Court also held that using testing and measuring methods as a hiring practice is still permitted as long as they represent a "reasonable measure of job performance."[26]

In 1973, the U.S. Supreme Court heard *McDonnell-Douglas v. Green*. This case clarified some discrimination provisions of Title VII. Specifically, it established guidelines for bringing a hiring discrimination case against an employer.

> *The complainant in a Title VII trial must carry the initial burden under the statute of establishing a prima facie case of racial discrimination. This may be done by showing (i) that he belongs to a racial minority; (ii) that he applied and was qualified for a job for which the employer was seeking applicants; (iii) that, despite his qualifications, he was rejected; and (iv) that, after his rejection, the position remained open and the employer continued to seek applicants from persons of complainant's qualifications.*[27]

The important point made here is that the burden is on the complainant. A person can't be discriminated against if they are not qualified for a position. A person can't be discriminated against if the employer opts *not* to fill the position.

In 1977, a class-action case was brought against Bowman Transportation Co. The holding in this case, also by the Supreme Court, established the Federal judiciary's authority to order remedies in Title VII cases. The Court stated that Title VII:

> *vests broad equitable discretion in the federal courts to 'order such affirmative action as may be appropriate, which may include, but is not limited to, reinstatement or hiring of employees, with or without back pay… or any other relief as the court deems appropriate.'*[28]

An interesting point the Court made in this holding centered on relief being granted to members of a class-action suit. The Court held that relief cannot be denied to members of a class (relief being awards such as back-pay or granting seniority) even though it could be construed as denying a benefit to employees not represented by the class or otherwise unaffected by the suit. In *Teamsters v. United States* in 1977, the Supreme Court again introduced the authority of the Federal judiciary to "make whole" any injured parties to a Title VII discrimination claim. The Court stated, "for a consistently enforced discriminatory policy can surely deter job applications from those who are aware of it and are unwilling to subject themselves to the humiliation of explicit and certain rejection."[29]

The 1980s

The 1980s began with *Texas Dept. of Community Affairs v. Burdine*, which was decided in 1981 by the Supreme Court. The Court stated that once a *prima facie* case of discrimination has been proven, the defendant's only burden is to explain how its actions were not discriminatory.[30] The Court cited *McDonnell-Douglas v. Green* in arriving at this decision, and further stated that the defendant did not even have to believe in its explanation; it had only to create a genuine issue of fact. The Court also held:

> *The explanation provided must be legally sufficient to justify a judgment for the defendant. If the defendant carries this burden of production, the presumption*

---

25 *Griggs v. Duke Power Co.* (401 US 424), 1971.
26 *Griggs v. Duke Power Co.*
27 *McDonnell Douglas v. Green* (411 US 792), 1973.
28 *Franks v. Bowman Transportation Co.* (424 US 747), 1977.
29 *Teamsters v. United States* (431 US 324), 1977.
30 *Texas Dept. of Community Affairs v. Burdine* (450 US 248), 1981.

> *raised by the prima facie case is rebutted, and the factual inquiry proceeds to a new level of specificity. Placing this burden of production on the defendant thus serves simultaneously to meet the plaintiff's prima facie case by presenting a legitimate reason for the action and to frame the factual issue with sufficient clarity so that the plaintiff will have a full and fair opportunity to demonstrate pretext.*[31]

Also noted is that if the defendant successfully offers an explanation for its conduct, the burden shifts back on the plaintiff (complainant). The plaintiff must then prove that the defendant is being dishonest regarding its actual reason for the alleged discriminatory act. As you can see, the Supreme Court has begun making more specific decisions regarding discrimination, which will directly affect decisions regarding sexual harassment law.

In 1983, the U.S. Supreme Court decided *U.S. Postal Service Board of Governors v Aikens*. In this case, the Board responded to the complaint with evidence that its actions were not discriminatory against Aikens. The Supreme Court, therefore, said:

> *Here, the District Court erroneously thought that respondent was required to submit direct evidence of discriminatory intent, and erroneously focused on the question of prima facie case rather than directly on the question of discrimination. The prima facie case method established in McDonnell Douglas was "never intended to be rigid, mechanized, or ritualistic. Rather, it is merely a sensible, orderly way to evaluate the evidence in light of common experience as it bears on the critical question of discrimination."*[32]

This had the effect of making the *McDonnell Douglas* test rather flexible. This opened the doors for a landmark case on sexual harassment, which was decided in 1986.

The case that defined sexual harassment case law, *Meritor Savings Bank v. Vinson*, was decided by the U.S. Supreme Court in 1986. First, the Supreme Court established that sexual harassment is harassment under Title VII. Second, it also stated that a "hostile environment" may exist because of the harassment and that too is actionable under Title VII.[33] The District Court that initially heard the case ruled that there must be an economic or other tangible injury to the plaintiff in order to rule that harassment had taken place under Title VII. The Supreme Court further pointed out that the language used in Title VII suggests that employers may, *in some cases*, be insulated from liability for actions taken by its employees.

> *Congress' decision to define "employer" to include any "agent" of an employer evinces an intent to place some limits on the acts of employees for which employers under Title VII are to be held responsible. In this case, however, the mere existence of a grievance procedure in the bank and the bank's policy against discrimination, coupled with respondent's failure to invoke that procedure, do not necessarily insulate the bank from liability.*[34]

This same District Court was rebuked by the Supreme Court for focusing on the "voluntariness" of the plaintiff's actions. The Supreme Court said that the plaintiff's actions were irrelevant to the claim at hand, specifically, that the plaintiff was forced to work in a hostile environment because of her sex. The Court drew much of its support from guidelines issued by the EEOC, which will be covered in another part of this chapter. It was actually the EEOC that defined "hostile environment" and "*quid pro quo*" harassment; it took the support of the Supreme Court to get employers' attention.

On a somewhat different subject, the case of *Wards Packing Co. v. Atonio*, which was decided in 1989 by the Supreme Court, deals with hiring practices. The Court ruled that a simple comparison of the percentage of two kinds of workers does not *in itself* constitute a *prima facie* discrimination case. The comparison should be made between one type of

---

31 *Texas Dept. of Community Affairs v. Burdine.*

32 *Aiken v. U.S. Postal Service Board of Governors* (460 US 711), 1983.

33 *Meritor Savings Bank v. Vinson* (477 US 57), 1986.

34 *Meritor Savings Bank v. Vinson.*

worker against the local labor pool as a whole. The absence of a demographic group at the workplace is not the fault of the employer if the demographic group is sparsely represented throughout the town, municipality, or county.[35]

In *Price Waterhouse v. Hopkins*, which was decided by the Supreme Court in 1989, mainly addressed the defenses an employer can use in a Title VII case. Cases decided in favor of a defendant in a Title VII complaint are not unusual; however, those that make it to the Supreme Court are quite rare. In this case, the Court held that the defendant can avoid liability if it can prove that it would have taken the same actions "in the absence of discrimination"; this is regardless of whether the plaintiff proves its case or not. "An employer is not deemed to have violated Title VII if it proves it would have made the same decision in the absence of an impermissible motive," said the Supreme Court.[36]

1990–1997

The 1990s saw the refinement of sexual harassment case law and the clarification of various issues. Little has changed in the three years of the 21st century in terms of case law. In 1993, the "hostile work environment" form of sexual harassment was clarified by the U.S. Supreme Court in *Harris v. Forklift Systems*. The Court had several holdings in this case, and complimented several items first introduced in *Meritor Savings Bank v. Vinson*.

In *Harris*, the Court said that a hostile work environment does *not* need to cause injury; it does not even have to have a demonstrable impact on a complainant's "well-being." It also established the "reasonable person" standard, stating that "This standard requires an objectively hostile or abusive environment—one that a reasonable person would find hostile or abusive—as well as the victim's subjective perception that the environment is abusive."[37] The Court also described the components that could make up a hostile environment complaint. The frequency of the discriminatory conduct is important; except in extremely rare cases, one or two incidences of discriminatory conduct are not sufficient to support a sexual harassment complaint. In order to support the hostile work environment claim, there must be numerous incidences, or the behavior must be persistent. The degree of offensiveness of the complaint must also be considered. Is the discriminatory behavior physically threatening to the victim? Is it "mere Page II offensive utterance"? Does it *unreasonably* interfere with work performance? No single factor is required, but all the circumstances surrounding the discriminatory behavior or behaviors should be examined.[38]

Also in 1993, the Supreme Court decided *St. Mary's Honor Center v. Hicks*. In this decision, the Court held:

> *This Court has no authority to impose liability upon an employer for alleged discriminatory employment practices unless the factfinder determines that the employer has unlawfully discriminated. Nor may the Court substitute for that required finding the much different and much lesser finding that the employer's explanation of its action was not believable.*[39]

Essentially, the possibility of the Court not believing the defense does not preclude the necessity for proving discrimination. If discrimination is not proven, then the defendant cannot be lying because the discrimination never occurred. The court further concluded that:

> *does if, on the evidence presented, (1) any rational person would have to find the existence of facts constituting a prima facie case, and (2) the defendant has failed to meet its burden of production—i.e., has failed to introduce evidence which, taken as true, would permit the conclusion that there was a nondiscriminatory reason for the adverse action.*[40]

---

35 *Wards Cove Packing Co. v. Atonio* (490 US 642), 1989.
36 *Price Waterhouse v. Hopkins* (490 US 228), 1989.
37 *Harris v. Forklift Systems Inc.* (510 US 17), 1993.
38 *Harris v. Forklift Systems Inc.* (510 US 17), 1993.
39 *St. Mary's Honor Center v. Hicks* (509 US 502), 1993.
40 *St. Mary's Honor Center v. Hicks*.

From 1994 to 1997, U.S. Courts of Appeal decided numerous Title VII cases. The 3rd and 4th Circuits decided three cases involving an employer's defense. The first, *Bouton v. BMW of North America*, was decided in 1994 by the 3rd Circuit, simply stated that an "effective grievance procedure, known to the victim, that timely stops the harassment is an effective shield against Title VII liability."[41] In 1996, the 4th Circuit heard *Andrade v. Mayfair Management*. In *Andrade*, the Court held that an employer is only liable for a sexually hostile work environment if the employer "knew or should have known" about the harassment *and* failed to remedy the problem in a reasonable and timely fashion.[42] Finally, in 1997, the 4th Circuit also heard *Hartsell v. Duplex Products* which indicated that Title VII sexual discrimination is based solely on the fact that the incidents occur because of the gender of the victim. Title VII does not promise civility in the workplace, but only a way to remedy an environment so miserable that a victim could not reasonably be expected to function there.[43]

The various Circuit Courts also provided guidance on the burden of proof in a Title VII action. In particular, the 7th, 8th, and 9th Circuits addressed these issues. In *Allen v. Bridgestone/Firestone Inc.*, decided by the 8th Circuit in 1996, the Court clarified the three-step process first introduced in *McDonnell-Douglas*. If the complainant satisfies those three steps, the burden shifts to the defendant to prove its actions against the complainant were not discriminatory. If the defendant satisfies that requirement, the burden shifts back to the complainant to prove that the defendant's explanation "was not pretextual."[44]

In 1997, the 8th Circuit decided *Gartman v. Gencorp*. In *Gartman*, the Court states the complainant must "show the conditions were intolerable." Further the Court required that in determining the level of intolerability, an objective standard must be used; the complainant's opinion alone is not sufficient. The complainant may prove constructive discharge "by showing their resignation was a reasonably foreseeable consequence of their employers' discriminatory actions."[45] Also in 1997, the 7th Circuit decided *Greenslade v. Chicago Sun Times*. In *Greenslade*, the Court held:

> *"If the employer presents no evidence that the plaintiff was not qualified or not treated less favorably, and offers no reason for the action taken against the plaintiff, then the plaintiff is entitled to judgment on the spot and so doesn't have to hazard a trial. If an employer articulates a legitimate, nondiscriminatory reason for its action, the plaintiff must "create an issue as to whether the employer honestly believes in the reasons it offers, not whether [the employer] made a bad decision."*[46]

The Circuit Appeals courts, of course, did not stop there. The 2nd, 8th, and 9th Circuits heard cases involving evidentiary issues in Title VII claims. In 1997, they decided two cases each regarding evidence. We begin with the 8th Circuit.

The 8th Circuit decided in *Kimzey v. Wal Mart Stores, Inc.* that a Title VII plaintiff may recover damages for any discriminatory act, provided any statute of limitations has not run out. It declared that evidence of incidents that occurred outside the statute of limitations can be admissible. A hostile environment claim may utilize such incidents to establish a pattern of discrimination.[47] Regarding a Title VII claim, the 8th Circuit stated that:

> *In a hostile work environment claim, evidence concerning all circumstances of the complainant's employment must be considered, including the frequency of the offending conduct, its severity, whether it was physically threatening or humiliat-*

---

41 *Bouton v. BMW of North America* (U.S. Court of Appeals, 3rd Circuit), 1994.
42 *Andrade v. Mayfair Management* (U.S. Court of Appeals, 4th Circuit), 1996.
43 *Hartsell v. Duplex Products* (U.S. Court of Appeals, 4th Circuit), 1997.
44 *Allen v. Bridgestone/Firestone* (U.S. Court of Appeals, 8th Circuit), 1996.
45 *Gartman v. Gencorp* (U.S. Court of Appeals, 8th Circuit), 1997.
46 *Greenslade v. Chicago Sun Times* (U.S. Court of Appeals, 7th Circuit), 1997.
47 *Kimzey v. Wal Mart Stores, Inc.* (U.S. Court of Appeals, 8th Circuit), 1997.

> *ing, and whether it unreasonably interfered with work performance. A workplace permeated with "discriminatory intimidation, ridicule, and insult" is sufficiently severe to establish a hostile work environment.*[48]

In addition, the Court ruled that if a complainant resigns because of a reasonable expectation that the situation will not improve, that constitutes "constructive discharge." The employer must provide a reasonable opportunity to resolve a situation prior to submitting a resignation. Offering an alternate job to a complainant may not shield the employer from liability.[49]

The 8th Circuit also heard *Delph v. Dr. Pepper Bottling Co*. In this case, the Court expanded on the concept of constructive discharge. The Court ruled that a constructive discharge occurs when an employer renders working conditions so intolerable that the employee feels no other recourse but to resign. The Court did provide a distinction in that "merely annoying" behavior would not result in a constructive discharge, but a "tangible psychological injury" suffered by the employee certainly would.[50] In addition, the Court made the following statement:

> *"Further, we have held that the employer's actions leading to the decision to quit must have been deliberate, that is, they must have been taken with the intention of forcing the employee to quit…Racial harassment directed at an employee by a single supervisor can sufficiently poison the employee's working atmosphere, since a supervisor can dominate the workplace with respect to his subordinate."*[51]

This statement goes a considerable distance in uniting the two different definitions of sexual harassment. *Quid pro quo* harassment is the obvious example of a supervisor "dominating the workplace" and having an effect on the working atmosphere as a whole. In this case, the Court was saying that even a hostile environment claim could be successful in court even when only one person was creating that environment.

The 9th Circuit, at the same time, heard *Yamaguchi v. Widnall* and the 2nd Circuit heard *Perry v. Ethan Allen*. In these cases, the Courts ruled that sexual harassment cannot be merely "episodic," it must be concerted to be considered pervasive. If harassment occurs because of coworkers (as opposed to supervisors or others), the employer will be held liable if the complainant can demonstrate the employer had ample opportunity to correct the harassment and failed to do so.[52] Additionally, during appeals, all evidence must be viewed in "the light most favorable to the nonmoving party." It must be determined if any issues of material fact exist and if the court of original jurisdiction applied the law appropriately. The Court further stated that a summary judgment is not sufficient if any factual issues exist.[53]

1998–2001

This section has been separated from "the 1990s" because the sheer volume of case law during this three-year period is considerable, and questions that reached U.S. Appeals Court Circuits and the Supreme Court were by this time more specific. Decisions regarding liability will be covered first.

In *Gallagher v. Delaney*, the 2nd Circuit acknowledged the vagaries of sexual harassment case law and the difficulty of some companies in determining how to respond to a harassment allegation without incurring some form of liability. The Court stated:

> *"If an alleged victim of sexual harassment asks a person of authority to whom she has reported the harassment to keep it confidential, and the employer attempts to reduce the emotional trauma on the victim by honoring her request, it risks liability for not*

---

48 *Kimzey v. Wal Mart Stores, Inc.*

49 *Kimzey v. Wal Mart Stores, Inc.*

50 *Delph v. Dr. Pepper Bottling Co*. (U.S. Court of Appeals, 8th Circuit), 1997.

51 *Delph v. Dr. Pepper Bottling Co*.

52 *Perry v. Ethan Allen* (U.S. Court of Appeals, 2nd Circuit), 1997.

53 *Yamaguchi v. Widnall* (U.S. Court of Appeals, 9th Circuit), 1997.

> *quickly and effectively remedying the situation… Too narrow a view of what is appropriate in reacting to an employee's conflicting needs for protection and for privacy may inhibit well-founded, valid complaints; too broad a view may unreasonably expand employers' duties beyond what Title VII requires and lead to unpleasantly gelid work environments. Lack of predictability of an ultimate jury reaction might cause employers and employees to be more formal in their workplace relationships than is necessary or desirable, in order to avoid any possible claim of sexual harassment."*[54]

This statement encompasses the difficulty in drafting a sexual harassment policy. Case law covering sexual harassment policies and their advantages or disadvantages is covered elsewhere in this chapter.

The next case is a State case, heard by the California Court of Appeals, 3rd District. In this case, *Department of Health & Human Services v. Sacramento County*, the Court held that vicarious liability exists when the harasser is a supervisor with immediate authority over the victim. If that supervisor did not cause or allow a "tangible" employment action, such as demotion, reassignment, or termination, then the company may still raise an affirmative defense. The Court in this case indicated a two-part test for the company to defend itself. The company must have a grievance procedure, and must be able to prove that the alleged victim did not follow it.[55]

Faragher v. Boca Raton, decided by the U.S. Supreme Court in 1998, dealt mainly with liability issues that deal with supervisors and/or managers. In a way, the Court ruled in this case that nothing is absolute; that an affirmative defense can be raised in a situation where a subordinate is sexually harassed by a supervisor. The Court does acknowledge also that the subordinate is not in the same position to respond to harassment as the same person would if the harasser was a coworker without supervisory authority. The Court stated, "An employer is vicariously liable for actionable discrimination caused by a supervisor, but subject to an affirmative defense looking to the reasonableness of the employer's conduct as well as that of the plaintiff victim."[56] In the same vein, the U.S. Court of Appeals, 8th Circuit, decided *Todd v. Ortho Biotech, Inc.* in 1998. In this case, the Court ruled that the employer is liable for sexual harassment if the perpetrator actually used supervisory authority to cause the harassment *and* if the supervisor does not use supervisory authority but it is known that he/she possesses such authority. The employer cannot take action afterward and be absolved of liability concerns.[57]

In a 5th Circuit case, *Indest v. Freeman Decorating*, the Court indicated a decision with two distinct parts. The first part involved the possibility that a *quid pro quo* Title VII complainant filing a lawsuit against both the supervisor (harasser) and the employer. The 5th Circuit ruled that this is not allowed. The employer would essentially be held liable twice for the same incident as it is responsible for the deeds of the supervisor, the doctrine of *respondent superior*.[58] The second part of the ruling involved the "level" of harassment in a Title VII complaint. The Court said, "Incidental, occasional or merely playful sexual utterances will rarely poison the employee's working conditions to the extent demanded for liability.…"[59] In a Utah case, the UT Court of Appeals ruled in *Autolive ASP v. UT Dept. of Workforce Services* that e-mail transmission of sexually offensive material, to include jokes, pictures, video, or other media will expose an employer to liability.[60] The various Courts still make a distinction between e-mail communication and verbal communication, even though the same standard could reasonably apply to both: "incidental, occasional, or merely playful.…"

In *Burrell v. Star Nursery*, the 9th Circuit affirmed the lower court's decision to grant summary judgment for the defense for part of the Title VII claim. The plaintiff, Burrell,

---

[54] *Gallagher v. Dulaney* (U.S. Court of Appeals, 2nd Circuit), 1998.

[55] *Department of Health & Human Services v. Sacramento County* (CA Court of Appeals, 3rd Circuit), 1998.

[56] *Faragher v. City of Boca Raton* (524 US 775), 1998.

[57] *Todd v. Ortho Biotech, Inc.* (U.S. Court of Appeals, 8th Circuit), 1998.

[58] *Indest v. Freeman Decorating* (U.S. Court of Appeals, 5th Circuit), 1999.

[59] *Indest v. Freeman Decorating*.

[60] *Autolive ASP v. UT Dept. of Workforce Services* (UT Court of Appeals), 2001.

alleged that Star Nursery was aware of, or should have been aware of, harassment taking place against her by both supervisors and managers. Through the trial and depositions, it was determined that Burrell had never complained to management, and that no management official had witnessed any harassing conduct. Therefore, the 9th Circuit ruled that Star Nursery would not be held liable for the actions of the coworkers and supervisors that allegedly harassed Burrell. The rest of the complaint was remanded back to the court of original jurisdiction for further action.[61]

In *Dees v. Johnson Controls*, the 11th Circuit established a test for determining vicarious liability against an employer. The Court stated that any of the following four theories are valid:

1) The supervisor holds such a high position in the Company that he could be considered the employer's "alter ego",
2) The harassment violates a "nondelegable" duty of the employer,
3) The supervisor uses "apparent authority" granted by the employer, or
4) The supervisor is aided in committing the harassment by the existence of his agency relationship with the employer.[62]

In the second theory, a "nondelegable" duty could be defined as that that cannot be passed along to a contractor. For example, a contractor may hire employees to work at a company, but once they are put under the authority of a company supervisor, the company is responsible for actions taken by that supervisor even as they relate to the contact employees.

The next three cases, all decided in 1998, involve employment actions. The first, *Burlington Industries v. Ellerth*, was decided in the Supreme Court. In this case, the Court ruled that the complainant can recover damages from an employer even though no tangible employment action occurred. Further, the complainant need not show that the employer was negligible. The Court also said, however, that the employer has a defense in this instance. The employer may have a defense *only* if no tangible employment action has occurred.[63]

The next two cases, *Draper v. Coeur Rochester* (9th Circuit) and *Reinhold v. Virginia* (4th Circuit), involve employment status. In *Reinhold*, the complainant filed suit after she rejected sexual advances made by her supervisor. In retaliation for her rejection, the supervisor began assigning her extra work. The Court ruled in this case that assignment of extra work, though unfair, is not a change in employment status.[64] A change in employment status would occur if she were terminated, demoted, or transferred. In *Draper*, the Court established when the statute of limitations begins on a constructive discharge complaint. In this case, the Court ruled that the limitation on filing a complaint begins on the date of discharge.[65]

Hostetler v. Quality Dining, Inc. was decided by the 7th Circuit U.S. Court of Appeals in 2000. The ruling in this case covered a variety of things. The Court began by stating that there is no "magic number" of incidents required to sustain a hostile environment claim. If the acts in question are physical in addition to verbal, there is still a "continuum." If a combination of innocuous touching and verbal comments occur, and the incidents are few and far between, then they will likely not be actionable.[66] The Court then stated that it recognizes that some remedial actions that are taken by employers that cause no reduction in their liability. The Court also said that,

> *"A transfer that reduces the victim's wage or other renumeration, increases the disamenities of work, or impairs her prospects for promotion makes the victim worse off. Therefore such a transfer is an inadequate discharge of the employer's duty of correction."*[67]

---

61 *Burrell v. Star Nursery* (U.S. Court of Appeals, 9th Circuit), 1999.
62 *Dees v. Johnson Controls* (U.S. Court of Appeals, 11th Circuit), 1999.
63 *Burlington Industries v. Ellerth* (524 US 742), 1998.
64 *Reinhold v. Virginia* (U.S. Court of Appeals, 4th Circuit), 1998.
65 *Draper v. Coeur Rochester* (U.S. Court of Appeals, 9th Circuit), 1998.
66 *Hostetler v. Quality Dining, Inc.* (U.S. Court of Appeals, 7th Circuit), 2000.
67 *Hostetler v. Quality Dining, Inc.*

Another case decided in 2000 called *Brooks v. City of San Mateo, CA* was heard in the U.S. Court of Appeals, 9th Circuit. In this case, the Court's ruling can be divided into two parts. The first part involves coworkers designated to hear sexual harassment complaints that are not members of management. The Court ruled that these persons, particularly if they are responsible for relaying complaints to managers that are not on-site, are considered "management" for the purposes of a Title VII complaint. In the second part of this ruling, the Court rules on liability issues for a company that has a situation like this. If the coworker that is notified of the complaint lacks the authority to address the situation, the employer will not be held liable unless that coworker has "an official or strong *de facto* duty to act as a conduit to management."[68]

The final two cases involve an employer's reaction, or lack thereof, to a harassment complaint. The first, *Rhieneck v. Hutchinson Technology*, was decided in 2001 by the U.S. Court of Appeals, 8th Circuit. In this case, the employer was granted summary judgment by the District Court. The plaintiff appealed and the 8th Circuit ruled that because the employer took every reasonable step to investigate and correct the complaint, and did so in a timely manner. The investigation into the complaint was started less than nine days after the complaint was filed. The employer interviewed ~30 people, removed a computer from the workplace that contained offending material and checked various others, redistributed the company harassment policy to all employees, and offered the plaintiff a transfer.[69] The second case, *Swenson v. Potter*, was decided by the U.S. Court of Appeals, 9th Circuit, also in 2001. In this case, the Court made rulings on several issues. It said that a discrimination complaint is considered "timely" only if the complainant has contacted an Equal Employment Opportunity (EEO) counselor within 45 days of the alleged incident. The Court further stated that in cases involving harassment by a coworker, the employer is only liable for its own actions or failures to act. The best defense an employer has in these situations is to promptly investigate the complaint. If the investigation is conducted in bad faith, that is attempting to reach a specific conclusion regardless of the facts at hand, it will not relieve the employer of responsibility in the matter.[70]

Schools, Colleges, Title IX

In 1986, a sexual harassment claim was brought involving a minor who gave a public speech to students attending a public school. The case, *Bethel School District v. Fraser*, was argued before the Supreme Court. In the ruling, the Court stated that the same latitude that applies to adults in a public forum does not necessarily apply to minors. The Court stated that under the First Amendment to the U.S. Constitution, the School District was not wrong for "determining that a vulgar and lewd speech such as respondents would undermine the school's basic educational mission."[71]

In 1998, the U.S. Supreme Court decided *Gebser v. Lago Vista Independent School District*. In this case, the Court ruled that there was a difference in the applications of Title VII and Title IX as they apply to the educational establishment. The Court stated that the relationship between supervisor and subordinate can be interpreted the same way as the relationship between teacher and student, as those relationships relate to a sexual harassment complaint. The Court made the distinction that Title VII is designed to compensate victims of discrimination while Title IX is intended to protect these victims from recipients of Title IX funding. The design of Title IX, further, assumes that a school official, when notified of a potential harassment claim, refuses to address the matter and return the school to compliance with Title IX. "We will not hold a school district liable for Title IX damages for a teacher's sexual harassment of a student absent actual notice and deliberate indifference…."[72]

---

68 *Brooks v. City of San Mateo* (U.S. Court of Appeals, 9th Circuit), 2000.

69 *Rhieneck v. Hutchinson Technology* (U.S. Court of Appeals, 8th Circuit), 2001.

70 *Swenson v. Potter* (U.S. Court of Appeals, 9th Circuit), 2001.

71 *Bethel School District v. Fraser* (478 US 675), 1986.

72 *Gebser v. Lago Vista Independent School District* (524 US 274), 1998.

The case *Davis v. Monroe County Board of Education* was decided by the U.S. Court of Appeals (11th Circuit) in 1999 and concerned student-on-student harassment in a public school. In this case, the Court made reference to the harassment taking place in a location "under the operation of a (Title IX) funding recipient."[73] The Court further stated that in this situation, the Board of Education exercises significant control over the harasser because the "nature of the state's power over public schoolchildren is custodial and tutelary, permitting a degree of supervision and control that could not be exercised over free adults."[74] As long as the harasser is under the Board's authority, at school, the Board incurs liability for failing to deal with student-on-student harassment if it becomes aware of it.

Equal Employment Opportunity Commission

The Equal Employment Opportunity Commission, commonly referred to as the EEOC, was created through the Civil Rights Act of 1964. It established a Commission with five members, all of whom are appointed by the president of the United States, with the "advice and consent" of the U.S. Senate.[75] The president also designates a chairman and vice chairman of the Commission. The chairman is the chief administrator of the Commission, and can appoint officers, agents, attorneys, administrative law judges, and other employees for the EEOC as needed.

The EEOC's powers are outlined in Title 42, Section 2000(e)(4) of the USC. The EEOC is authorized to cooperate with and utilize consenting local, regional, and State government agencies and individuals in furtherance of its mission. The EEOC can authorize studies that will "effectuate the purposes and policies of this subchapter and to make the results of such studies available to the public."[76] The EEOC is even allowed to intervene in a civil action brought under Section 2000(e)(5) by any party other than a government, government agency, or political subdivision.[77]

The procedure by which complaints are submitted, heard, and resolved by the EEOC is outlined in Title 42, Section 2000(e)(5) of the USC. The EEOC is authorized to prevent any unlawful employment practice as defined in Title VII and discussed earlier in this book.[78] A complaint about an unlawful employment practice can be filed by an individual, by an individual on behalf of someone else, by the EEOC, or by the EEOC on behalf of someone else. The EEOC notifies the accused of the complaint and must include the date, place, and events the complaint(s) refers to. The EEOC must make this notification within 10 days and is charged with investigating the complaint.[79]

Any complaint must be made "under oath or affirmation," meaning that a person could be charged with perjury for lying in a complaint before the EEOC. The complaint must contain any information and be presented in proper form as determined by the EEOC. The complaint cannot be leaked to the public.[80]

An EEOC complaint must meet the standard of reasonable cause. If a complaint is determined not to meet the reasonable cause standard, it is dismissed and both the complainant and the accused are promptly notified of the dismissal. If a complaint is determined to be true, the EEOC must first use "informal" methods to resolve the situation. The EEOC must determine the validity of the complaint within 120 days of the filing of the complaint.

"Informal" methods include conference, conciliation, and persuasion. The EEOC cannot make public any details involving an "informal" attempt to resolve a complaint nor can any details be used in subsequent complaints as evidence without written consent from both

---

73 *Davis v. Monroe County Board of Education* (U.S. Court of Appeals, 11th Circuit), 1999.
74 *Davis v. Monroe County Board of Education.*
75 42 USC 2000(e)(4)(a).
76 42 USC 2000(e)(4)(g)(1).
77 42 USC 2000(e)(4)(g)(6).
78 42 USC 2000(e)(5)(a).
79 42 USC 2000(e)(5)(b).
80 42 USC 2000(e)(5)(b).

parties. The penalty for releasing such information is a fine of less than $1,000.00 and/or imprisonment for less than one year.[81]

Although this fact is frequently glossed over in news reports about sexual harassment complaints filed through the EEOC, the law in Section 2000(e)(5) specifically says that complaints that occur in a

> *"State, or political subdivision of a State, which has a State or local law prohibiting the unlawful employment practice alleged and establishing or authorizing a State or local authority to grant or seek relief from such practice or to institute criminal proceedings with respect thereto upon receiving notice thereof, no charge may be filed under subsection (a) of this section by the person aggrieved before the expiration of sixty days after proceedings have been commenced under State or local law, unless such proceedings have been earlier terminated, provided that such sixty-day period shall be extended to one hundred and twenty days during the first year after the effective date of such State or local law."*[82]

That was somewhat long-winded, but that it means is that a complaint *must* have been filed with a State or local authority if a law exists in that State, region, or municipality that prohibits the alleged conduct. The complaint filed locally does not have to be resolved prior to filing with the EEOC, but it must be initiated on the State or local level **and** the complainant must wait 60 days to file with the EEOC. If the law prohibiting the alleged conduct was enacted in the year the complaint was filed, the waiting period is extended to 120 days. The intention of this waiting period was twofold—(1) it was to allow any other complaint time to be processed prior to the EEOC taking action, and (2) It was to force complaints to be heard elsewhere so that the EEOC could function as a "court of last resort" for complaints made in a State or local jurisdiction as opposed to a Federal one. Incidentally, the reason that the EEOC would want to allow time for other complaints on an incident to be processed is also found in Section 2000(e)(5). It states that when the EEOC is determining "reasonable cause," it must "accord substantial weight to final findings and orders made by State or local authorities in proceedings commenced under State or local law."[83]

The EEOC also reserves the right to file a civil complaint against any respondent, except a government agent or entity, if the EEOC cannot informally settle a complaint either 30 days after a charge is filed with the Commission or 30 days after the expiration of any deadline imposed in Section 2000(e)(5). If this same situation occurs with a government agent or entity, the same time limits apply but a civil complaint *will not* be filed by the EEOC. The complaint, instead, will be filed by the Attorney General in the appropriate U.S. District Court.[84] The implication of these statements is that once an individual decides to file a complaint with the EEOC, the complaint is no longer under their control. If an agreement between the aggrieved parties is not reached, the EEOC can file suit independently.

If a charge is filed with the EEOC and the EEOC concludes after investigation that "prompt judicial action is necessary," the EEOC may try to obtain temporary or preliminary relief pending the disposition of the complaint. Any such attempt is governed by Rule 65 of the Federal Rules of Civil Procedure.[85] Rule 65 reads as follows:

> ***Rule 65. Injunctions***
>
> (a) PRELIMINARY INJUNCTION.
> (1) Notice. No preliminary injunction shall be issued without notice to the adverse party.
> (b) TEMPORARY RESTRAINING ORDER; NOTICE; HEARING; DURATION.

---

81 42 USC 2000(e)(5)(b).
82 42 USC 2000(e)(5)(b).
83 42 USC 2000(e)(5)(b).
84 42 USC 2000(e)(5)(f)(1).
85 42 USC 2000(e)(5)(f)(2).

A temporary restraining order may be granted without written or oral notice to the adverse party or that party's attorney only if:

(1) it clearly appears from specific facts shown by affidavit or by the verified complaint that immediate and irreparable injury, loss, or damage will result to the applicant before the adverse party or that party's attorney can be heard in opposition, and
(2) the applicant's attorney certifies to the court in writing the efforts, if any, which have been made to give the notice and the reasons supporting the claim that notice should not be required.
(d) FORM AND SCOPE OF INJUNCTION OR RESTRAINING ORDER.

> *"Every order granting an injunction and every restraining order shall set forth the reasons for its issuance; shall be specific in terms; shall describe in reasonable detail, and not by reference to the complaint or other document, the act or acts sought to be restrained; and is binding only upon the parties to the action, their officers, agents, servants, employees, and attorneys, and upon those persons in active concert or participation with them who receive actual notice of the order by personal service or otherwise."*[86]

Obviously, each situation is different. Rule 65 lays the groundwork for obtaining a temporary injunction or restraining order. These orders can be granted with or without notice, depending on circumstances. However, any restraining order or injunction will give the reason for the order and explain specifically what act(s) is prohibited.

29 CFR 1601 Through 29 CFR 1611

In addition to the items covered in Title VII regarding the creation and operation of the EEOC, there are also parts of Title 29 of the Code of Federal Regulations that govern the EEOC, specifically, Sections 1601–1610.

29 CFR 1614

In 42 USC 2000(e), the statute excludes political appointees, elected officials, government agencies and departments, and other political subdivisions from Title VII coverage. In order for the EEOC to regulate these exempted bodies, Title 29, Section 1614 of the Code of Federal Regulations was created.

Section 1614 specifically includes any military department but exempts uniformed military personnel, which are covered under the Uniform Code of Military Justice. Section 1614 also includes all executive departments, the U.S. Postal Service, Postal Rate Commission, Tennessee Valley Authority, all competitive service positions in the Judicial branch, the National Oceanic and Atmospheric Administration Commission Corps., the Government Printing Office, and the Smithsonian Institution. Oddly enough, Section 1614 also lists departments that are excluded from this regulation, such as the Library of Congress, the General Accounting Office, and alien (noncitizen) employees of the Federal government.[87]

Liability

Having defined *sexual harassment*, the next thing that must be defined is *liability* as it relates to this issue. Both of these definitions are based on statutory and case law at the time of this writing. The State and local laws regarding *sexual harassment* and *liability* may vary from place to place. In *Forbidden Grounds*, a book by Richard Epstein, he states, "In a *quid pro*

---

[86] Rule 65, Federal Rules of Civil Procedure. December, 2001, pp. 74–75.
[87] 29 CFR 1614.103.

quo case, the corporate defendant is strictly liable for the supervisor's harassment…when a supervisor requires sexual favors as *quid pro quo* for job benefits, the supervisor, by definition, acts as the company." Epstein notes that this liability standard is for *quid pro quo* harassment only. What this means to the security manager is that the employer could be successfully sued even if the employer, other than the instigating supervisor, had no knowledge that the harassment occurred. This is because the supervisor is considered to be acting within the scope of his or her duties. Regarding hostile environment harassment, Epstein writes, "In a hostile environment case, no *quid pro quo* exists. The supervisor does not act as the company; the supervisor acts outside 'the scope of actual or apparent authority to hire, fire, discipline, or promote'." What this means to the manager is that a suit against the employer for sexual harassment may not be successful because the supervisor is acting outside his or her duties. In summation, Epstein states, "corporate liability, therefore, exists only through *respondeat superior*; liability exists where the corporate defendant knew or should have known of the harassment and failed to take prompt remedial action against the supervisor."[88] In simpler terms, where the supervisor is directly involved in the harassment, both the supervisor and the company are liable. In cases where the supervisor is not directly involved in the harassment, but ignores it or fails to stop it, the supervisor is liable but the company is not, unless the company also was aware of the harassment.

Most of the applicable case law on the subject of *sexual harassment* and *liability* comes from a landmark Supreme Court decision from 1986; the case of *Meritor Savings Bank v. Vinson* (477 U.S. 57). In *Meritor*, the Court made several decisions that have established precedent in sexual harassment cases. In the decision, it was stated that:

> *"In that case, the EEOC believes, agency principles lead to:*
> *a rule that asks whether a victim of sexual harassment had reasonably an avenue of complaint regarding such harassment, and, if available and utilized, whether that procedure was reasonably responsive to the employee's complaint. If the employer has an expressed policy against sexual harassment and has implemented a procedure specifically designed to resolve sexual harassment claims, and if the victim does not take advantage of that procedure, the employer should be shielded from liability absent actual knowledge of the sexually hostile environment (obtained, e.g., by the filing of a charge with the EEOC or a comparable state agency)."*[89]

Transfer/Insurance

One of the remedies that have arisen since the early 1990s is what is referred to as *employment practices liability coverage*, or EPL. Basically, it is insurance against lawsuits charging unlawful employment practices such as sexual harassment. "Five years ago, premiums for companies with fewer than 100 employees were in the $50,000 to $100,000 range. Today, premiums on the same policy might run an employer $5,000." Originally, few insurers would allow coverage against these suits. Now, however, large companies such as "Chubb, Lloyds of London, and Reliance offer EPL." This has caused the cost of EPL to "plummet."[90]

Another remedy that was pioneered in 1988 by the E. I. DuPont de Nemours and Company (DuPont), based in Wilmington, Delaware, is to have a program that addresses and explains sexual harassment. DuPont's program is called "A Matter of Respect." This is a class, typically 4 hours long, that is offered frequently and usually involves 20–25 employees, plus 2 facilitators. During the class, the employees watch videotapes of situations, and they are then called on to determine if each situation would be considered harassment. They discuss the issue among themselves until they come up with an answer. The facilitator asks

---

[88] Richard A. Epstein (1992). *Forbidden Grounds*. London, England: Harvard University Press, p. 363.

[89] *Meritor Savings Bank v. Vinson*, 477 U.S. 57 (1986).

[90] Shaheena Ahmad, p. 61.

the employees some questions and makes some statements to assist them in their analysis.[91] Currently, 65% of DuPont's employees have participated in the program.

The program goes far beyond the class that is offered. The facilitators offer a list of their names, phone numbers, and a list of other internal contact people, should an employee wish to discuss "any of the issues or problems they're having in more detail."[92] The facilitators of the program receive 5–30 days of training, which allows them to counsel other employees and to be involved in the initial investigation of any complaints. They learn to talk to worried employees as well as listen to them.[93]

Investigation

Investigation is the key to determining if there is a valid complaint, determining what actions need to be taken against a harasser, and preventing litigation. The most important thing about investigating a sexual harassment complaint is to do it immediately. "A prompt and objective investigation should be the standard response to any complaint of sexual harassment"[94] in order to decrease liability.

Investigating all possible instance of harassment, regardless of how they come to the employer's attention, reduces the potential for liability.[95] Provided the employer already has a policy against sexual harassment, the employer must then designate a person or persons that can hear sexual harassment complaints and act on them without bias, preferably someone in a different chain of command than the complainant. The security manager can be that person; however, the security manager should have alternate people to perform investigative duties in the event when there is a conflict. Conflicts would include personality conflicts with the complainant or the alleged harasser. It may even become necessary to hire an independent investigator.[96]

From there the investigation should begin. The investigator should attempt to get whatever information possible from the complainant, the alleged harasser, and witnesses. The information should include:

1) The identity of the person(s) accused of the offensive action and any witnesses to the alleged harassment;
2) What specific conduct is objectionable;
3) How many times and over what period of time the conduct has occurred;
4) Whether any other employees have experienced this type of offensive conduct;
5) Whether there have been any previous complaints to fellow employees, the harasser, or others about the offensive conduct; and
6) Whether there is any pattern to the offensive conduct.[97]

The objectives for the investigation should also be clear. Know **why** an investigation is being initiated, and **what** is intended to come because of it. The manager by initiating an investigation should:

1) Determine whether a basis of fact exists to formally accuse the employee
2) Serve, if an accusation has already been made, as the basis of fact for determining if the accusation was warranted, and if warranted, as the basis for initiating some type of discipline

---

91 Gillian Flynn (October, 1997). A pioneer program nurtures a harassment free workplace. *Workforce*, pp. 38–40.

92 Flynn Gillian, p. 40.

93 Gillian Flynn, p. 41.

94 Bryan A. Chapman, Recommended guidelines for the employer. Available: http://www.baclaw.com/# promptly and objectively, p. 6.

95 Karen Sutherland (1997). Investigating Sexual Harassment Claims – What's a Business Owner To Do? Available: http://www.omwlaw.com/pubs/sutherland/00014.html, p. 1.

96 Karen Sutherland, p. 2.

97 Karen Sutherland, p. 2.

3) Serve, if some type of disciplinary action has been effected, such as a suspension from duties pending the outcome of an investigation, as the basis for either sustaining or rescinding the action
4) Determine if a basis of fact exists for imposing discipline over and above what already may have been given relative to the misconduct investigated[98]

There are even recommended guidelines for interviewing individuals that have relevant knowledge to the complaint being investigated. They are:

1) Disclose information only on a need-to-know basis.
2) Ask broad and open-ended questions that are not limited to the specific facts of the complaint. Let the alleged victim know that they employer takes the matter seriously and will promptly investigate it.
3) Take notes and follow up on any leads that the questioning reveals, even if they are not directly or specifically related to this complaint.
4) Conduct the interview in a non-threatening environment, in a manner that encourages the interviewee to be forthcoming. If the interviewee feels uncomfortable, probe gently or return to the question or subject later in the interview.
5) Remind interviewees that there will be no retaliation for participating in this interview.[99]

Occasionally, there are witnesses to the harassment. This is especially so if the case regards a hostile environment. If a complaint is being investigated, there will probably be witnesses involved. When a security manager decides to include witnesses in his or her inquiry, that manager should consider the following:

1) If the allegations are such that the accused will likely admit to them, you may want to postpone your witness interviews. Then, if all material allegations are admitted, your employer may not see a need to involve potential witnesses.
2) If the material allegations are denied, then you have an unresolved factual dispute, and witness interviews are needed to attempt to resolve the dispute.[100]

In cases where the accused does not admit to the allegations, but instead denies them, it is entirely possible that the accused is not telling the truth. If the security manager suspects that the accused is lying, that manager may wish to consider these options:

1) Cease interviewing and proceed directly into an interrogation. Conduct this in accordance with acceptable interrogative techniques you would use in any other type of investigation.
2) Commit the accused to a false exculpatory statement. The value of such a statement is that it is documentary proof of deception. Such a statement is based on the accused denying facts that can be proven true.
3) Carry out both of the above suggestions: If the interrogation fails to produce a confession, a false exculpatory statement can then be obtained.[101]

Sometimes, the investigation does not clearly state if the alleged harasser did commit the action for which he or she has been accused. This is not uncommon. If this is the case, inform the harasser that if the additional evidence surfaces at a later time, the investigation will be reopened and appropriate action will be taken.[102]

---

[98] Louis V. Imundo (1985). *Employee Discipline: How To Do It Right*. Belmont, CA: Wadsworth Publishing Company, p. 76.

[99] Karen Sutherland, p. 2.

[100] Michael E. Connell (December, 1987). How to investigate sexual harassment. *Security Management*, p. 35.

[101] Michael E. Connell, p. 35.

[102] Karen Sutherland, p. 2.

Discipline

If the employer has determined that sexual harassment did take place, then disciplinary action must occur. Otherwise, the investigation and the efforts of various people will have been wasted.

One of the most important things to remember about disciplining people is to be "objective and consistent."[103] For discipline to be effective, it must correct the act, not belittle the person. The discipline that is given should depend on the offender's previous behavior. Keeping a file on employee infractions, that is, to document each violation and keep that information sorted by employee/offender allows the record to be easily accessed to determine if the offender is a repeat offender or if he or she has committed other violations.[104] If action is to be taken, in order to be effective it must be taken promptly. If there is a time lapse between the offense and the disciplining, then the offender may not recall why he or she is being disciplined. That practice would cause low employee morale. Also, when disciplining, the manager should remember that "the discipline should fit the severity of the conduct and be calculated to immediately put a stop to the offensive conduct."[105]

One option that may be used to discipline an employee is termination from employment. If the employee is found to have committed sexual harassment after an investigation, the safest course of action would be to fire that person. This is not always practical, however. If alternative forms of discipline are to be utilized instead, certain things should be considered:

1) determine the presence and degree of guilt prior to disciplining
2) because of intense emotions surrounding a sexual harassment accusation, be careful to separate fact from fiction as emotion will distort an employee's claims
3) sexual harassment **could** be symptomatic of an emotional illness; medical treatment could be considered for use as constructive discipline
4) there must be a well-communicated sexual harassment policy in existence prior to the accusation
5) understand that things said in jest may not be similarly interpreted. In determining the degree of guilt, motive is as important as what was actually said or done[106]

Consideration must also be given to the possibility of false accusations. As sexual harassment has expanded over the years to include female-on-female, male-on-male, and female-on-male sex harassment, the possibility of someone's behavior being classified as sexual harassment has increased tenfold and with it the possibility that someone might falsify accusations for personal, monetary, or employment gains. False reporting should be treated as seriously as a sexual harassment offense itself. The possibility of a lawsuit from a wronged innocent employee or former employee would be just as embarrassing to the company as a lawsuit from a wronged employee.

Conclusion

Even though much relevant information on sexual harassment has been stated here, laws and court decisions continually change the way that the issue is viewed. The best way to ensure that sexual harassment is avoided is to have a clear and concise policy on the subject, and to be sure that the policy is updated periodically to include any changes made by the courts or by Federal, State, and local legislative actions. Once policy has been established, adhere always to the procedures that have been outlined and update them when necessary. Have corporate

---

[103] Charles A. Sennewald (1985). *Effective Security Management*. Boston, MA: Buttwerworth Publishers, p. 111.

[104] Charles A. Sennewald, p. 112.

[105] Karen Sutherland, p. 2.

[106] Louis V. Imundo, p. 242.

counsel reviewed any policies and procedures to ensure compliance with whatever applies in the local, State, and Federal jurisdiction *where the facility is located?* If a company has facilities in multiple states, the policies may have to differ, sometimes substantially. Where possible, attempt to eliminate the problem, not the employee. Finally, remember **confidentiality** above all things. Sexual harassment accusations, be they true or not, are extremely damaging to all concerned.

Sexual Harassment

Questions

1. Whats ection of Federal law covers the statutory definition of sexual harassment?
   a. 19 USC 1595(a)
   b. 42 USC 2000(e)
   c. 8 CFR 214.2(a)
   d. 18 USC 229

2. What was the popular name of the act that created 42 USC 2000(e)?
   a. Tariff Act of 1930
   b. Family & Medical Leave Act
   c. Civil Rights Act of 1964
   d. Sexual Abuse Act of 1986

3. Sexual harassment is considered, by Federal law, to be an unlawful employment practice in every situation.
   a. True
   b. False

4. The term "Employee," as defined in Title VII, *does not* include which of the following persons:
   a. Stock Clerk at the local Wal-Mart
   b. The Mayor of Syracuse, NY
   c. Delivery Truck Driver for Coca-Cola®
   d. Engineer for General Motors®

5. Title IX protections were created to extend the reach of Title VII. These protections cover:
   a. Schools, Colleges, and Universities
   b. 4-H
   c. International Order of Hibernians
   d. International Association of Odd fellows

6. The Commonwealth of Massachusetts has a sexual harassment law that regulates the following:
   a. Establishing training programs to combat sexual harassment
   b. Establishing policies against sexual harassment
   c. Determining how often a company must communicate sexual harassment policy to its employees
   d. All of the above

7. The landmark Supreme Court case regarding sexual harassment law is cited as:
   a. *Faragher v. City of Boca Raton*
   b. *Franks v. Bowman Transportation Co.*
   c. *Aiken v. U.S. Postal Service Board of Governors*
   d. *Meritor Savings Bank v. Vinson*

8. The term "hostile environment" as it relates to sexual harassment first appeared in which case:
   a. *Meritor Savings Bank v. Vinson*
   b. *Wards Cove Packing Co. v. Antonio*
   c. *Harris v. Forklift Systems*
   d. *Gartman v. Gencorp*
9. Can a person bringing a discrimination claim under Title VII recover damages?
   a. Yes
   b. No
10. If you resign from your job because of sexual harassment, could you bring suit against your employer alleging 'hostile environment'?
   a. Yes
   b. No