SECURITY
BUSINESS PRACTICES REFERENCE

6

Physical Security
Investigations
Emergency Planning
Safeguarding Proprietary Information
Personnel Security
Security Management

ASIS International

Security
Business Practices Reference

6

Professional practices for security managers
seeking to improve security within their organizations

ASIS Council on Business Practices

published by ASIS International
Alexandria, Virginia

1625 Prince Street, Alexandria, VA 22314
www.asisonline.org

Benefit from the Experience of Colleagues

Sir Isaac Newton said, "If I have seen further, it is by standing on the shoulders of giants." Likewise, you—the security professional—can benefit from studying the work of your security colleagues. By collecting examples of specific, successful experiments in security problem solving, this document will help you build on your colleagues' experiences, standing on their shoulders and seeing further, as you look to solve security challenges in your own enterprise.

What You Will Find

Through actual case studies, the authors present a problem that occurred, the response taken to correct that problem, and the results achieved when the response was implemented. In some cases, the solution provided measurable results, which are depicted in a chart or graph. Contact information is included with each case so you can communicate with the author directly to learn more about the cited problem or solution.

How to Use This Book

To gain the most from *Security Business Practices Reference, Volume 6*, begin with a review of the table of contents. The case studies are divided into six core topics, which replicate the domains used in the Certified Protection Professional (CPP) designation. The topics are defined broadly, and often cases could fit in more than one topic area.

Acknowledgments

Published by ASIS International (ASIS), *Security Business Practices Reference, Volume 6*, was compiled by a subcommittee of the ASIS Council on Business Practices. Chaired by Joseph DiDona, the subcommittee included Glen Kitteringham, Jerry Loghry, and Tony Vermillion. Peter Ohlhausen, president of Ohlhausen Research, Inc., and a former editor of *Security Management* magazine, edited and produced the document. Special thanks are given to the security professionals who submitted the business practices in this volume.

Note: The business practices presented in this book reflect the good faith efforts and actions of security practitioners. The publisher does not certify their reliability.

CONTENTS

PHYSICAL SECURITY

Industry	Employees	Yearly Revenue
Mining	1,600	$200,000,000

Cutting Warehouse Theft

The Problem

The problem was employee theft of items from a warehouse. The physical structure and layout of the warehouse was not designed with security in mind. Therefore, it was a virtual buffet for dishonest warehouse personnel and mechanics, who were freely allowed access into the warehouse. Warehouse supervisors were writing off an average of 100 items per month. Most items taken were of modest value, but the sheer volume of what was missing added up. Making the situation worse was the fact that the operation lies in a remote location in the middle of Central Asia, where obtaining supplies takes time and money. A missing 25-cent bolt has the potential to shut down a multimillion-dollar operation.

The Solution

The first step was to restrict access to authorized personnel only. This was accomplished by formulating a written warehouse access control policy and procedure. To further control access, card swipe readers were installed at each door and only authorized personnel were issued with access cards. The database that tracks who enters and exits and when is audited daily by the security superintendent.

Next, a part return policy was initiated. For example, if a mechanic requires a carburetor for a work order, he must first bring in the carburetor that needs to be replaced. Old items are locked in a sea container for later disposal.

Closed-circuit television (CCTV) cameras were installed, both fixed and pan-tilt-zoom. A security control room for the monitor and recording device is manned on a 24/7 schedule.

The Outcome

Since the installation of the access control and CCTV equipment, along with the procedural changes, monthly write-offs have dropped by 68 percent. There have been neither operational shutdowns nor a drop in vehicle availability due to parts not being available.

Robert F. Marcelain, CPP
Corporate Security Manager

Kumtor Operating Company
24 Ibraimov St.
Bishkek, Kyrgyzstan 720031

996 612 600707
robert_Marcelain@kumtor.com

Industry	Employees	Yearly Revenue
Armored Transportation	4,000	$250 million

Enhancing Secure Storage Methods

The Problem

An armored car company transported valuables to its facility for overnight storage in highly secure vaults. For greater security, the vaults could only by opened by two people working together, using a system called "dual control." The company's compliance officers discovered instances in which combination holders shared their combinations with each other, thereby eliminating the system of dual control. Vault combinations could potentially be comprised once employees started deviating from company policy.

The Response

To ensure that dual control policies were followed, the company equipped the vault doors with new locks, the combinations of which are changed daily. To obtain a combination, two employees must call the company's alarm central station. Central station monitors verify the identity of each employee, and if they are authorized to open the vault, one combination is issued to each employee. Each combination must be entered using a preset electronic key assigned to a specific employee. The vault can only be opened after both employees enter the combinations they were given. The information used to identify each employee is destroyed once the employee leaves the company. The company also plans to use remote monitoring through the alarm central station to visually verify the identity of the two employees requesting the lock combinations.

The Outcome

The new system—supplying employees daily with new vault combinations linked to their personal electronic keys—has provided an added layer of security for the armored car company. Since installing the new locking system in the company's branches, compliance officers no longer have to look for employee sharing of combinations. Two individuals are now required to be present, and an alarm system employee outside the branch knows whenever a vault door is opened. With the total reinstatement of dual control, any potential duress situations would be uncovered before the valuables inside the vault were exposed. The company's insurance underwriters are pleased that the company has implemented an innovative security program that protects not only the valuables stored overnight but also the company's employees.

James L. Dunbar, CPP
Chairman

Dunbar Armored, Inc.
50 Schilling Rd.
Hunt Valley, MD 21031

(410) 229-1929
james.dunbar@dunbararm.com

Industry	Employees	Yearly Revenue
Healthcare	2,400	$300 million

Guest Registration Program

The Problem

St. Jude Hospital employees invite a number of business guests to the hospital each day to participate in training and research activities and to demonstrate the latest technology in both clinical and non-clinical fields. As a rule, the Security Department is not aware of who the guests are or when they are arriving. Because St. Jude Hospital has a controlled-access campus with four vehicle gates, all these invited guests are delayed at the gates while the security officer verifies the purpose of their visit, logs them in, and issues them a vehicle pass.

The Response

The Security Department, in collaboration with the Information Technology Services Department, developed a form that is available to our employees on the St. Jude intranet. The program is loaded on each employee's desktop for easy access. The employee completes the form and sends it to the Security Department, thereby providing advance notification of when a guest is due to arrive. The form includes the name of the guest, the date and time of the visit, the gate the guest will be entering, and the person who will be the visitor's host. The Security Department prepares a printed ID badge, which is waiting for the guest when he or she arrives at the gate.

The Outcome

As a result of this initiative, the Security Department has advance notification of when business guests are coming. The guest registration program does the following:

- allows the department to expedite the check-in process
- makes visitors feel special because a printed ID badge with their name and their company's name has been prepared before their arrival
- helps identify visitors while they are in the hospital

The program is expanding as more and more departments become familiar with the process.

Robert T. Haas, CPP
Director of Security

St. Jude Children's Research
Hospital
332 N. Lauderdale St.
Memphis, TN 38105

(901) 495-3352
robert.haas@stjude.org

Industry	Employees	Yearly Revenue
Commercial Real Estate	681	$9 billion

Insecure Doors

The Problem

Gulf Canada Square is a Class A commercial high-rise building in Calgary, Alberta, Canada. Located in the downtown core, the property has massive floor plates of up to 85,000 square feet. The 22-story structure is about 1.1 million square feet in size and has roughly 3,000 occupants.

For years, the downtown core has been prey to thieves, especially laptop thieves. Displaying no building attack pattern, the culprits have proven themselves quick and smart, generally entering through insecure doors. Security practitioners know that doors found insecure more often than others become easy targets for repeated attacks. However, the victims generally believe that (a) security stops all problems at the front door to the building, (b) the cleaners will secure the space, (c) security is on-site, so the building must be secure, and (d) no one is dishonest. To victims, their insecure doors are not the issue—only the theft is.

An audit showed that cleaners, tenants, contractors, service providers, and even base building staff were all contributing to the problem, creating the ideal environment for thieves. The audit also revealed that effective management of the mechanical aspect of the doors themselves was necessary. Card access system schedules, door locks and closures, hardware, electric strikes, and electromagnetic locks all came under close scrutiny. Although security staff regularly locked the insecure doors, recording and monitoring was sporadic at best.

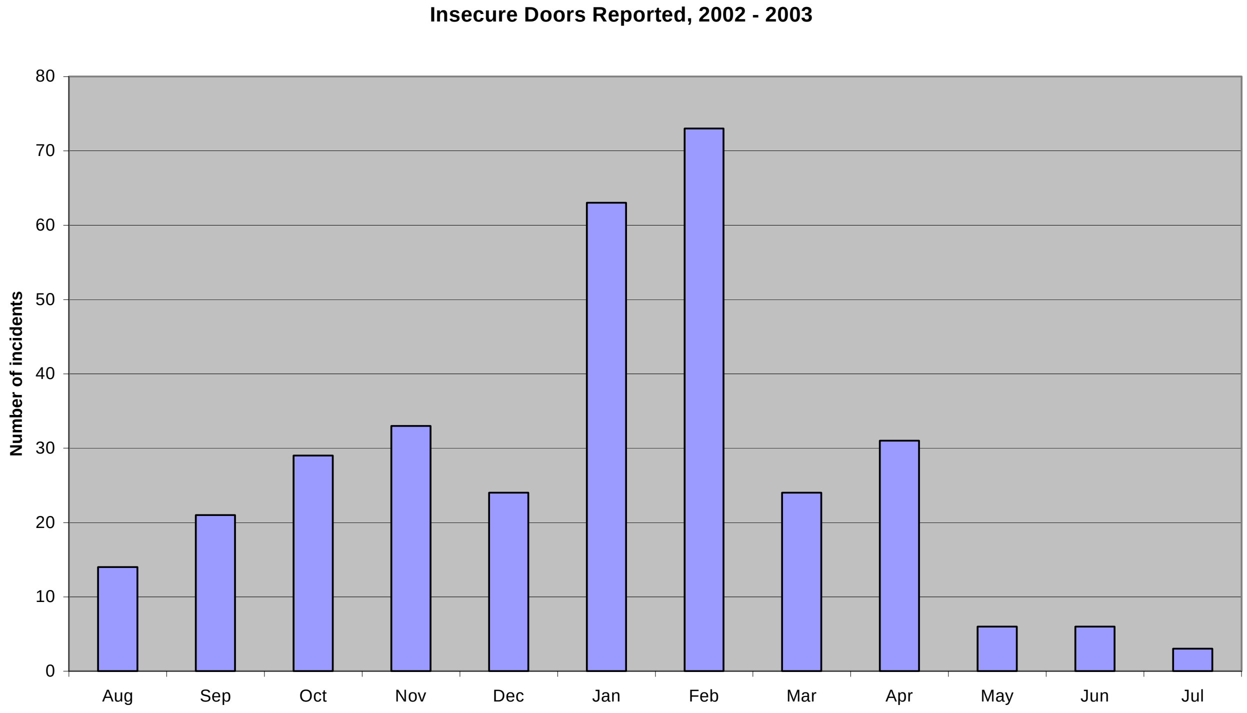
The Response

Security management introduced a “doors found open” program and monitored the number of insecure doors reported each day. Even the doors to base building mechanical rooms, riser rooms, and washrooms were monitored. Door reports included the cause (left unlocked, hardware/mechanical problems, time schedules, etc.) and corrective action taken.

Tenants, contractors, building maintenance, and cleaners were informed of the findings. An awareness campaign was begun, using posters, bulletins, and e-mail. In addition, in the monthly security/tenant meetings, insecure doors became part of the regular agenda.

The Outcome

The education and awareness program demanded that everyone take ownership of the solution. That effort, along with the “doors found open” reporting, demonstrated almost immediate results. The graph on the following page indicates the number of insecure doors found before and after the program was initiated in March 2003.



Gina Arbeau
Coordinator, Security & Life Safety

Brookfield Properties Corporation
Suite 185, 401–9th Ave. SW
Calgary, Alberta, Canada T2P 3C5

(403) 221-1155 (fax)
garbeau@brookfieldproperties.com

Industry	Employees	Yearly Revenue
Commercial Real Estate/ Property Management	650+	$8.2 billion

Office Tower Skateboarders

The Problem

Located in Calgary, Alberta, Petro Canada Centre is a Class AA, 2.1 million square foot multi-tenant, commercial, twin tower high-rise. It is one of the most sought-after premises in the city. Unfortunately, this reputation extends to both desirables and undesirables alike.

For many years, the site has suffered from the attention of skateboarders due to its uniquely designed plaza. Some of the skateboarders—a few "bad apples"—occasionally broke into cars or into restaurants in the food court area or stole or damaged property. Some tenants were uncomfortable in the plaza area, which saw regular skateboarding activity—as many as 40 skateboarders on a weekend afternoon. Damage to the benches, handrails, curbs, and planter area was estimated at $10,000 a year. In addition, approximately $15,000 a year was spent on extra security officers, regular officers responding to incidents, and officers documenting activities. The annual cost to the Centre was thought to be approximately $25,000.

The Response

The first step was to measure the problem. Starting February 1, 1999, and continuing to this day, security officers began recording the number of skateboarders on-site. Additional security officers were hired in spring 1999 for the summer months to provide a continual presence to deter skateboarders and document the extent of their site visits. It was determined that the site was visited by some 2,800 boarders a year. In 2001, when a downtown skateboard park opened, the number dropped to 2,300. Unfortunately, in 2002, the numbers were back up to over 2,800.

Property management coordinated a multi-pronged response, replacing benches with individual metal seats, cutting notches in the marble to reduce grinding areas, adding signage, setting large planters and garbage cans in the way of skateboard runs, conducting constant patrols, and continually removing the skateboarders from the area. Recognizing that the issue could affect other buildings, a number of property owners in the downtown core joined forces, conducted a survey to determine the extent of the problem, and then met with city officials, police, and parks and recreation staff regarding enforcement issues. City officials responded by rewriting the bylaw dealing with skateboarders, giving police and bylaw officers the authority to seize skateboards. The bylaw change generated media attention, which alerted skateboarders to the new penalty.

The Outcome

As a result of the considerable response activities, the numbers of boarders seen at Petro Canada Centre in 2003 was down 55 percent year-to-date (Jan.-June) in comparison to the numbers seen between 1999-2002. Security management feels the reduction will persist. From a historical perspective, 60 percent of all incidents occur in the first six months of the year. This 60 percent translates into a cost of $15,000. A 55 percent reduction is valued at $8,250 for the first six months of 2003. That savings is only the hard cost. Soft costs have been reduced now that there is increased tenant satisfaction, less time spent by security officers dealing with skateboarders, an enhanced building reputation, reduction of breaking and enter and car prowling, and a decrease in negative interactions between security and undesirable visitors.

Skateboarders Observed

	1999	2000	2001	2002	2003
Jan.	0	83	301	315	67
Feb.	0	131	68	490	56
Mar.	650	247	40	196	269
April	670	315	236	286	135
May	357	322	238	290	146
June	280	568	183	220	69
July	170	454	254	236	
Aug.	320	392	292	234	
Sept.	273	257	325	262	
Oct.	55	48	231	138	
Nov.	75	10	125	61	
Dec.	14	2	95	81	
Total	2864	2829	2386	2809	742

Glen Kitteringham, MSc, CPP
Senior Manager, Security & Life Safety

Brookfield Properties
Fifth Avenue Place, Suite 101, 420–2nd St. SW
Calgary, Alberta, Canada T2P 3K4

(403) 770-2363
gkitteringham@brookfieldproperties.com

Industry	Employees	Yearly Revenue
Semiconductor Equipment	5,000 (U.S., Europe, Asia)	$1.5 billion

Site Facility Security Maturity Model

The Problem

The security department was unable to quickly demonstrate two security issues to company executives:

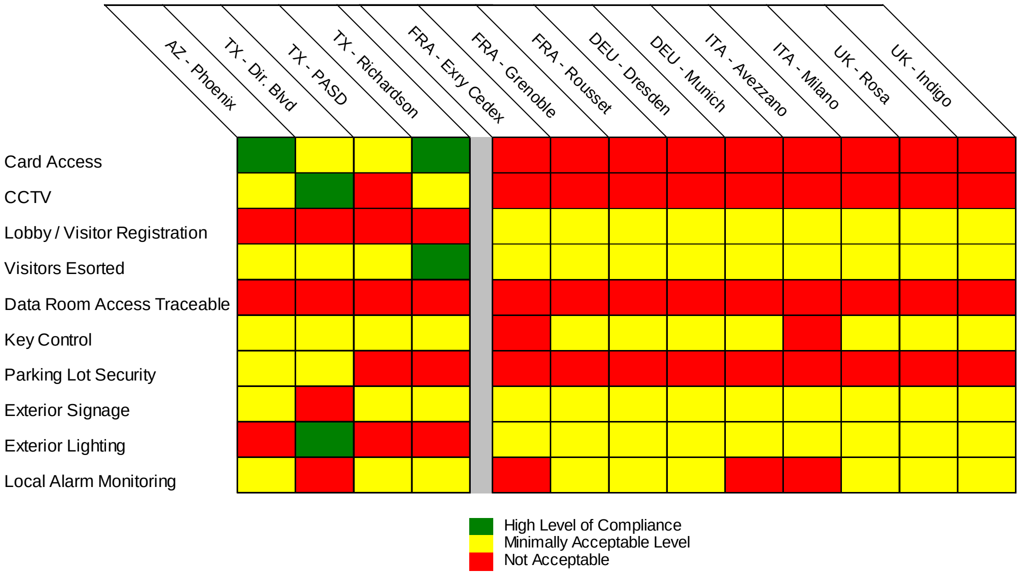
- the company's physical security needs
- the progress of a 52-building security systems upgrade throughout the United States, Europe, and Asia

The Response

A physical security assessment questionnaire was developed and sent to the manager responsible for each building. The questionnaire covered the core components of the company building security standards. For example, each manager was asked whether all physical keys were accounted for and recorded and whether the building was equipped with access control, CCTV, or intrusion alarm systems.

For each core component, each manager was also asked to rank the level of compliance or degree of acceptance from 1 to 5 (1 being unacceptable and 5 being "meets company security standards"). Security management assigned a red, yellow, or green color code to each question, based on the manager's ranking. A maturity model graph was created by listing the core components of the company building security standards in the left column and the facility locations along the upper row (see charts). The color code, or level of maturity, was placed at the corresponding cell of the building location and the core security component.

July 2002 Scorecard – Partial US and Europe



	AZ - Phoenix	TX - Dir. Blvd	TX - PASD	TX - Richardson	FRA - Exry Cedex	FRA - Grenoble	FRA - Rousset	DEU - Dresden	DEU - Munich	ITA - Avezzano	ITA - Milano	UK - Rosa	UK - Indigo
Card Access	🟩	🟨	🟨	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
CCTV	🟨	🟩	🟥	🟨	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Lobby / Visitor Registration	🟥	🟥	🟥	🟥	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Visitors Esorted	🟨	🟨	🟨	🟩	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Data Room Access Traceable	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Key Control	🟨	🟨	🟨	🟨	🟥	🟨	🟨	🟨	🟨	🟥	🟨	🟨	🟨
Parking Lot Security	🟨	🟨	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Exterior Signage	🟨	🟥	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Exterior Lighting	🟥	🟩	🟥	🟥	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Local Alarm Monitoring	🟨	🟥	🟨	🟨	🟥	🟨	🟨	🟨	🟥	🟥	🟨	🟨	🟨

🟩 High Level of Compliance
🟨 Minimally Acceptable Level
🟥 Not Acceptable

July 2003 Scorecard – Partial US and Europe

	AZ - Phoenix	TX - Austin (Rialto)	TX - PASD	TX - Richardson		FRA - Corbeil Essonnes	FRA - Grenoble	FRA - Rousset	DEU - Dresden	DEU - Munich	ITA - Avezzano	ITA - Milano	UK - Rosa	UK - Molly Millars
Card Access	🟩	🟩	🟥	🟩		🟥 I	🟩	🟩	🟩	🟥 I	🟥 I	🟩	🟩	🟩
CCTV	🟩	🟩	🟩	🟩		🟥 N	🟩	🟩	🟨	🟥 N	🟥 N	🟩	🟩	🟨
Lobby / Visitor Registration	🟨	🟨	🟨	🟨		🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟩	🟨
Visitors Esorted	🟩	🟨	🟩	🟩		🟨 P	🟨	🟨	🟨	🟨 P	🟨 P	🟨	🟩	🟩
Data Room Access Traceable	🟩	🟩	🟥	🟩		🟥 R	🟩	🟩	🟩	🟥 R	🟥 R	🟩	🟩	🟩
Key Control	🟩	🟩	🟨	🟩		🟥 O	🟨	🟨	🟨	🟨 O	🟥 O	🟩	🟩	🟩
Parking Lot Security	🟩	🟩	🟨	🟩		🟥 C	🟨	🟨	🟩	🟥 C	🟥 C	🟩	🟨	🟨
Exterior Signage	🟩	🟩	🟨	🟩		🟨 E	🟨	🟨	🟨	🟨 E	🟨 E	🟨	🟨	🟨
Exterior Lighting	🟩	🟩	🟨	🟩		🟨 S	🟨	🟨	🟨	🟨 S	🟨 S	🟨	🟨	🟨
Local Alarm Monitoring	🟩	🟩	🟨	🟩		🟥 S	🟩	🟩	🟩	🟥 S	🟥 S	🟩	🟩	🟩

🟩 High Level of Compliance
🟨 Minimally Acceptable Level
🟥 Not Acceptable

The Outcome

The resulting maturity model provided security management and company executives a one-page graphical display of the buildings, grouped by geographic regions, and any core security components (clearly identified in red) that did not meet company security standards. The maturity model also served as a useful tool for developing the project roadmap. Changes in the graphs from quarter to quarter reflected the progress of the 52-site security systems upgrade. The maturity model was updated each quarter and presented to company executives.

Jeff Gurulé, CPP
Corporate Security Manager

KLA-Tencor Corporation
160 Rio Robles
San Jose, CA 95134

(408) 875-6164
jeff.Gurule@kla-tencor.com

INVESTIGATIONS

Industry	Employees	Yearly Revenue
Information Technology Services	316,303	$88 billion

Industrial Espionage

The Problem

A multinational corporation with headquarters in the United States and offices spread around the world suffered repeated attempts at industrial espionage. Unidentified persons were trying to obtain sensitive information about the company's internal organization. They were also trying to get technical support material for the company's new service offerings. On one occasion, an attempt concerned sensitive information prepared to support a specific bid, which was ready to be presented to an important customer. Several individuals, all working for the same organization, attacked subsidiaries of the corporation in a number of countries, attempting to steal information by posing as headhunters or consultants. There was no evidence of hacking activities or information and communication technology (ICT) security breaches.

The Response

The corporation suspected that a major competitor was behind the plot and, consequently, activated all available means to combat the problem.

Investigations were begun as soon as management in a medium-sized Asian country reported a fraudulent attempt to obtain corporate information via a fax machine. A couple of country security organizations contacted the company's Global Corporate Security Department. A structured reporting procedure was quickly set up, and within a few weeks valid evidence was being gathered. There were several attempts daily against the corporation, showing a very aggressive attack against sensitive information located in the different localities where the corporation was operating. Within three weeks, after collecting evidence of matching occurrences, it was surmised that all the attempts were being carried out by the same person or organization.

Investigations led to a small employment consulting firm, located in a very pleasant town in the south of Italy, and a lady who, reciting the role of headhunter and hiding behind her native English speaking capability, disguised her real intent.

All the available detailed information was filed according to date, geography, modus operandi, and call-back phone or fax number. Once the origin of the hoax calls and other activities had been identified, a warning letter was sent to the suspected firm. There was no response, so a couple of official reports were filed with the local police authority, which decided to interview an individual suspected of being the head of the criminal activity. No criminal charges were brought at that time.

The day the most direct effort was made to obtain corporate information, on-line monitoring was activated. The attempt was partially rebuffed and fully monitored. All evidence (including phone numbers and e-mail IDs) was officially reported to the competent judicial authority.

The Outcome

If the case had not been successfully investigated, the company would have lost its $48 million bid, which was already at an advanced stage of negotiations. As it turned out, the investigation was successful and the bid was won.

Finally, the suspected firm was taken to court and stands accused of being behind the criminal calls. It is also charged with extracting, by means of deceit, vital proprietary information belonging to the victim corporation.

The trial, which is ongoing, has brought to light information suggesting that other corporations may be victims of the same offender. They, too, will probably defend their rights in court.

This case has shed light on a serious and dangerous phenomenon that could damage several organizations. Fraudsters presenting themselves as aggressive headhunters or employment consultants manage to gather information which, when pieced together with other intelligence, gives them and their clients an insight into the private sphere of corporations.

As result of this problem, numerous tutorials have been given to company executives and administrative assistants, who are most exposed to this type of threat.

Alessandro Lega, CPP
Senior Partner and Consultant

INSIGNA Security Organization
Corso di Porta Nuova, 2
20121 Milano, Italy

+39 02 2900 1918
alessandro_lega@tin.it

EMERGENCY PLANNING

Industry	Employees	Yearly Revenue
Commercial Real Estate	650+	$8.2 billion

G8 Summit Security Planning

The Problem

Since the World Trade Organization riots in December 1999 in Seattle, Washington, a number of high-profile world events, including the annual G8 Summit meetings, have degenerated into chaos. Rioting and looting have led to numerous injuries and millions of dollars' worth of property damage and security costs.

G8 Summit meetings are the annual gatherings of eight industrial nations, including the United States, Canada, France, Great Britain, Russia, Japan, Italy, and Germany. Such a meeting was scheduled to take place in June 2002 in Kananaskis Country (known as K-Country), a park area approximately 100 kilometres or 60 miles from Calgary, Alberta, Canada. Because K-Country is far from the city and was to be guarded by several thousand members of the Canadian military and the Royal Canadian Mounted Police, the concern was that protesters would more likely voice their protests in downtown Calgary, a city of almost 1 million.

The Response

In anticipation of the summit, several property management organizations and major oil and gas companies met in January 2002. They decided to plan collectively instead of making security arrangements individually. Over the next six months, membership swelled from 18 members to 230, from both the public and private sectors, and the group held nine meetings. At those planning sessions, presentations were made on a number of strategies, and responses were suggested and discussed. Police, emergency medical service, and fire officials spoke on bomb threat response, dealing with protesters, medical response to discharge of tear gas and pepper spray, and hazmat response to chemical or biological releases. Police resources included a real-time e-mail fan-out system to disseminate information pertinent to all listed members.

Private organizations created mutual aid strategies; systems for rapid dissemination of critical information, such as location, direction, and size of protest groups; rapid shutdown of building HVAC (heating, venting and air conditioning) systems; rapid lockdown of buildings; and strategies for dealing with protesters and reduced access into buildings. Further, private security organizations were given a forum for discussing potential security officer supply problems as the G8 Summit date moved closer.

The Outcome

Unlike many recent international meetings, the G8 Summit, held June 26-27, 2002, was not marred by injury to anyone or destruction of any private property. While geography had a considerable impact on protesters, or the lack thereof, the preparation and planning, along with the relations developed between various organizations and between the private and public sectors, was of tremendous benefit. As a result, protests were a very minor aspect of the summit, which was acclaimed a success by both event organizers and city officials.

Glen Kitteringham, MSc, CPP
Senior Manager, Security & Life Safety

Brookfield Properties
Fifth Avenue Place, Suite 101, 420–2nd St. SW
Calgary, Alberta, Canada T2P 3K4

(403) 770-2363
gkitteringham@brookfieldproperties.com

SAFEGUARDING PROPRIETARY INFORMATION

Industry	Employees	Yearly Revenue
Insurance	14,500	$1.2 billion

Information Protection Plan for Telecommuting Employees

The Problem

As healthcare insurance companies look for opportunities to reduce selling, general, and administrative (SG&A) costs by consolidating personnel functions and cutting facilities, more employees are working from home. Telecommuting employees now work in sales and marketing, claims processing, underwriting, human resources, and other specialties. According to the U.S. Department of Labor, in 2002 some 28 million American workers telecommuted three or more days a week from home. However, telecommuting puts proprietary information at risk. Because of the lack of controls and poor security awareness, such information—whether in electronic, hard copy, or oral form—is vulnerable to compromise by competitors, house guests, and other preying eyes. Raising the stakes, the Health Insurance Portability Accountability Act (HIPAA) requires health insurance companies to protect subscribers' private health information (PHI) through de-identification procedures and tighter data controls. As telecommuting increases, so does the amount of proprietary data discarded in household trash. Among the data may be social security numbers, medical reports, and financial information.

The Response

To reduce the potential for data theft or misuse in telecommuting situations, a healthcare insurance company implemented a three-layer approach with the following elements:

- *Information Protection Agreement (IPA).* An employee who is approved for telecommuting and will conduct official business at home must read and sign an agreement that charges the employee with responsibility for such corporate assets as computers, software, and official documentation while working off-site. The employee also agrees to unannounced on-site audits by the corporate audit and security department to ensure compliance with required controls. The agreement is signed each year and placed in the employee's personnel file.

- *Self-Managed Controls.* The company provides or funds the equipment needed to safeguard internal information at the telecommuter's residence. Such equipment includes a shredding machine; computer equipped with anti-virus, firewall, and encryption software; and fax machine if needed. Each piece of equipment bears an asset tag, the number of which is recorded on the IPA.

- *Telecommuting Risk Assessment Program.* The audit and security department conducts an audit at the home once a year, using the following instrument:

Controls	Findings
Is the information protection agreement current and on file in Human Resources?	**Yes/No**
Does the IPA have a complete and accurate listing of corporate assets at the assignee's residence?	**Yes/No**
Is there a designated part of the residence dedicated to official business? • Is the dedicated room accessible to the outside? • Is there adequate protection on all external entrances?	**Yes/No** **Yes/No** **Yes/No**
Are documents in trash baskets not shredded as required?	**Yes/No**
Is the protection software activated and updated in the computer?	**Yes/No**
Are there signs of official data stored on unapproved computers?	**Yes/No**
Is there unapproved software on the corporate computer?	**Yes/No**
Are there data backups of work records? Are they properly secured?	**Yes/No**
Are business documents stored outside of the designated area of business? • If so, has it been approved by Risk Management? • Is there an inventory asset tracking report on file for those items stored? • Has the storage area been assessed by Audit/Security for adequate protection?	**Yes/No** **Yes/No** **Yes/No** **Yes/No**
Is the corporate confidentiality statement on all documents, including correspondence?	**Yes/No**
Is the assigned computer properly password protected?	**Yes/No**

The Outcome

The telecommuting information protection plan was implemented over a two-year period. It reduced improper data handling and document management by 75 percent, as measured by the results of the risk assessment and other site visits by management. Violations identified during visits were documented, and they resulted in disciplinary action and revocation of work-at-home privileges. They also affected employees' annual performance reviews. Telecommuters were given "information protection awards" for visits and risk assessments that showed strong control compliance. The program has been driven as a prevention program and is focused not on catching employees being noncompliant but rather on strengthening data protection off-site.

Steven I. Adler
Audit Manager

Health Net, Inc.
P.O. Box 270272
West Hartford, CT 06127

(860) 416-0620
sadler@ne.health.net

Industry	Employees	Yearly Revenue
Government	2,600	$3.5 billion+

Information Security Program Metrics

Problem

In 2003, the Connecticut Department of Social Services (DSS), recognizing the need for a comprehensive information security program, created the position of information security officer. DSS is the largest state agency in Connecticut, operating more than 90 state- and federally-funded programs that provide essential services to the residents of the state. The security program needed to consider the various forms of sensitive data (healthcare, financial, tax, personnel records), interagency relationships, and outsourced entities. A security risk assessment was performed and an information security program was designed and implemented at the agency.

The problem was how to determine how well the information security program was working. To manage the program with limited resources, it would be necessary to acquire statistical information that would highlight areas of weakness or non-compliance with both state and federal regulations.

Response

An analysis was performed to derive a common set of metrics that would be captured to reflect performance. This baseline consisted of the following:

- incorrect login attempts
- viruses/trojans received
- IT security certifications and accreditations
- review and analysis of audit trails
- physical security incidents
- business continuity/disaster recovery testing
- critical application testing
- security awareness testing
- system scans
- policy (non-compliance) incidents
- Web-based attacks
- internal incidents
- external audits

A review of the regulatory requirements (of, for example, the Health Insurance Portability and Accountability Act, Centers for Medicare and Medicaid Services, and Internal Revenue Service) and guidelines helped refine these metrics. Consideration was also given as to what results should trigger an investigation or a request for an audit.

Outcome

By evaluating the security metrics, DSS executive management could more easily determine the trends and note areas that were progressing slowly. For example,

- A low frequency of audits being performed on DSS information systems reflected a staffing issue.

- The absence of business continuity/disaster recovery testing indicated that plans were no longer being maintained.

- Increases in physical security incidents were usually related to budget issues (regarding, for example, monitoring, access controls, or security officers).

- An overall rise in policy violations indicated the need for security awareness training.

- IT operations incidents were often the result of inadequate or nonexistent processes or procedures.

The DSS information security officer considered security metrics to be a valuable tool for communicating the “state of security” and obtaining the necessary support to fix security-related problems.

Bernard Alexander Collins,
CPP, CISM, CISSP, CBCP
Information Security
Manager/Consultant

3528 Barron Berkeley Way
Raleigh, NC 27612

(919) 788- 0399
cci-security@ieee.org

Industry	Employees	Yearly Revenue
Financial	6,000	undisclosed

Modem/Analog Line Abuse Prevention

The Problem

In a "war-dialing" audit for a medium-sized financial institution, 750 modem/analog telephone line combinations were identified. This was 20 percent higher than anticipated, based on the documentation at the time. Immediate initiatives were undertaken to understand the unexpected growth and the prescribed versus actual use of the modems/analog lines. It was determined that a large number of the devices had been used solely to contact non-corporate Internet service providers. The use of a "personal" Internet service provider allowed employees to skirt corporate e-mail monitoring and content analysis tools. This allowed for the transmission of sensitive or proprietary data and the downloading of hazardous files without corporate intervention. Hazardous files, running the gamut from viruses to pornographic material, that are downloaded to the corporate PC held the potential for propagation through the network.

The Response

A policy was immediately developed to explain acceptable uses of modem/analog line setups, along with approval policies and procedures. Scope, definitions, scenarios, business impact, and enforcement were key elements of the policy.

A Web-based mechanism was designed and put in place to provide employees who felt they needed a modem/analog line setup with a method of justifying their request. Likewise, the mechanism allowed for the justification of existing configurations.

An exhaustive audit was performed of all modem/analog line devices and their traffic records. All lines demonstrating unequivocal abuse were immediately removed.

Memos were sent to managers responsible for all remaining modem/analog line devices. The memos gave them 30 days to justify the business case for keeping the devices. Configurations without an acceptable business case were removed on the 31st day.

The Outcome

The company has established an infrastructure policy to deal with the auditing, acquisition, removal, monitoring, and enforcement of modem/analog line configurations. By removing over 100 unjustified phone lines, the company saved more than $60,000 in annual charge-back costs and line tolls.

Loftin C. Woodiel, PhD, CPP
Principal Security Consultant

Woodiel & Associates
24 Victoria Dr.
Granite City, IL 62040

(618) 931-7973
professeurwoo@aol.com

Industry	Employees	Yearly Revenue
Publishing	1,000+	$2.4 billion

Reducing Laptop Thefts

The Problem

Over a period of 18 months, a single-tenant office building with over 1,000 employees and contractors had been experiencing an unusual amount of laptop thefts. As a security department best practice, patrols were initiated to determine the incidence of unsecured laptops. It was determined that 90 percent of laptop computers were unsecured. The company had no evident policy concerning the safeguarding of laptops at the time.

The Response

Looking further into the situation, the security and information security departments came up with a solution to reduce the theft of company laptops from employees' offices.

The Information Security Department provided all laptop users with a cable-locking device and key, as well as training and initial installation. Training was supplemented with locking instructions left with the users. All users were required to sign an acknowledgement form upon receipt of the locking device. Acknowledgment forms were filed along with the backup key in a secure location accessible to only the Information Security Department.

In addition, a policy was developed requiring that laptops be secured at all times. During the office day, they must be locked in docking stations or secured with the cable-locking device. Outside the office, they are to be secured using the provided locking device. An employee must secure the key and serial number of the locking device not in plain sight of the locking device. An employee is expected to protect the asset as if it were his or her own.

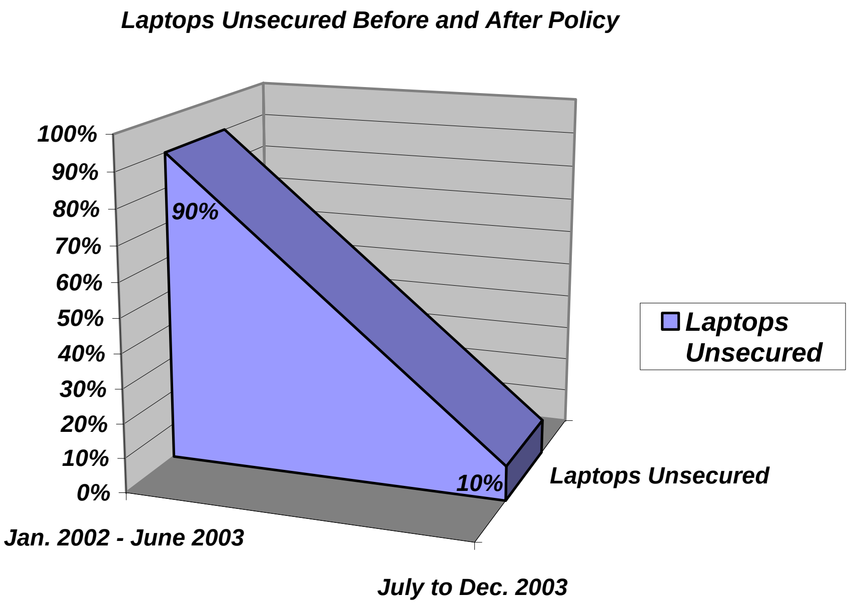
The Corporate Security Department periodically checks offices to ensure that laptops are secured. The first time a laptop is found unlocked, the user is issued a security violation notice and the security staff member issuing the notice records the incident. One copy of the violation notice is left on the unsecured laptop, and the other is delivered to a security coordinator, who logs the information for appropriate follow-up. The Information Security Department is notified via e-mail when laptops are found unsecured and follows up to see whether the user needs a locking device.

The second time a laptop is found unlocked, it is removed and the user must personally come to the security office to retrieve it. To minimize impact on company operations, unsecured laptops that are found processing are not removed. Instead, the security staff member secures the laptop where it is, using a cable-locking device. The user receives a violation notice and must pick up the key in the security office.

If the key for the cable locking device is found within plain sight of the laptop, the key is used to secure the laptop, and then the key is confiscated. The user receives a violation notice and must pick up the key in the security office.

The Outcome

The company policy that has been put into action has deterred the theft of laptops. Over a period of six months, compliance with the policy has been positive. The chart below shows that from 2002 through June 2003 more than 90 percent of laptops were unsecured. After administering the policy from July to December 2003, less than 10 percent were found unsecured. This policy not only deters laptop theft but also informs and safeguards company employees, equipment and documents.



Halbert G. Villagomez
Security Supervisor

Reader’s Digest Association, Inc.
Reader’s Digest Road
Pleasantville, NY 10570

(914) 244-5121
Halbert.Villagomez@rd.com

PERSONNEL SECURITY

Industry	Employees	Yearly Revenue
Technology	6,000	$3.7 billion

Establishing a Global Intelligence Website for Company Travelers

The Problem

A large scientific company conducts business throughout the world and has facilities in more 24 countries. In 2002, its employees made approximately 12,000 business trips: 7,000 domestic, 5,000 outside the United States. It was becoming a daunting task for the Travel Department to keep up with the latest travel warnings issued by the U.S. Department of State, intelligence from the Overseas Security Advisory Council, the latest acts of terrorism, and threat warnings. Company travelers relied on outside sources in assessing risk while considering a destination or when preparing for departure. In a post-9/11 environment, it was difficult to distribute information to the traveling population, and the timeliness and accuracy of global intelligence were difficult to assess.

The Response

In April 2003, the company sought to obtain threat assessment data from vendors in the field in order to mitigate the risk faced by company travelers. After issuing requests for proposals and conducting due diligence, including site visits to appropriate vendors to assess their capabilities and staff, the Corporate Security Department conducted in-house beta testing of products and services. A numerical scorecard was developed to weigh the strengths and weakness of each vendor. At the company's request, three vendors granted 90-day trial subscriptions to their threat assessment products and services.

The Outcome

The vendor assessment, including the beta testing, scorecard evaluation, and site visits, was completed in July 2003. A quality vendor was chosen to provide threat assessment data, flight and airport analysis, executive protection support, global intelligence, and other travel enhancements. Additionally, the vendor helped the company develop an intranet website that includes information about company sites worldwide, such as directions, hotels, restaurants, and up-to-date intelligence about risks associated with travel. Travelers can obtain destination information by clicking on a world map that shows locations where the company has facilities and employees. The website is also available in several different languages to appeal to a greater audience. Much additional security-related information is also available via a drop-down menu. Topics include what travelers should do if they lose their wallets or passports, how to protect laptops, news from the security director, currency conversion, and links to other security sites. In the first month alone, the website recorded 445 hits. It will continue to help company employees reduce their travel-related risk.

Richard Lagg, CPP
Corporate Security Manager

lagg1@mindspring.com

Industry	Employees	Yearly Revenue
Mining	1,600	$200,000,000

Expatriate Turnover Due to Security Concerns

The Problem

The company's operation is located in Central Asia, not far from Afghanistan. Shortly after the terror attacks of September 11, 2001, the company began to experience increased turnover among its expatriate employees. Many wished to resign or not renew their employment contracts.

In conducting exit interviews with these personnel, the corporate security manager learned that in the great majority of cases, the reason behind their decisions was fear of a terrorist attack, either while in country or in transit to North America.

The Response

The company could not afford to continue losing highly skilled and experienced personnel. However, management also realized that the employees had a legitimate concern. The company developed a plan to increase expatriate employees' comfort level and to gain their trust and confidence—that is, to make clear that the company would look after them and ensure their safety to the best of its ability.

The response included these elements:

- Communication and close ties with the appropriate government and diplomatic missions had to be established or reestablished. Those contacts would provide the company with up-to-the-minute threat assessments and information regarding the region and air travel routes.

- A weekly security update report was distributed via e-mail to all expatriates and their spouses, explaining the current security situation.

- An open-door policy was started, and all personnel were encouraged to contact the security manager with any security concerns or rumors that might be circulating.

- Informational meetings were held to explain various aspects of the company's crisis management plan. The intent was to demonstrate that the company had prepared itself for any crisis.

- Quarterly tabletop exercises of the crisis management plan were conducted with the crisis management team members.

The Outcome

No more expatriates have resigned or failed to renew an employment contract due to security concerns. Everyone realizes that the threat is still there, but they now feel more comfortable because they are kept in the communication loop. They also feel the company is taking all necessary actions to ensure their safety.

Robert F. Marcelain, CPP
Corporate Security Manager

Kumtor Operating Company
24 Ibraimov St.
Bishkek, Kyrgyzstan 720031

996 612 600707
robert_Marcelain@kumtor.com

Industry	Employees	Yearly Revenue
Banking	134,000	$10.8 billion

Lobby Management Training to Reduce Bank Robberies

The Problem

A banking company's branch locations in the Sacramento, California, area were being robbed at an increasing rate.

The Response

The regional corporate security manager provided a robbery training program for bank managers and assistant managers. After a non-security regional executive saw the program and learned of security measures employees could take to respond to and even prevent bank robberies, overtime pay hours were authorized so the staff at each branch could stay after closing hours to hear the security presentation, which corporate security tailored to each site.

The security manager spent the next few months attending after-hours staff meetings at each branch in the region, presenting a training program that included bank robbery preparedness, response, and familiarization. In addition, the presentation included a new segment on aggressive lobby management for robbery prevention. Instead of waiting to see if a potential suspect showed a note or pulled a gun after reaching a teller window, employees were taught to develop their awareness and observation skills, recognize suspicious persons, and aggressively approach both normal customers and suspicious persons to alter the course of events.

In one scenario, a suspect stood in a branch lobby, not quite waiting in line but close enough to be seen by staff on the platform. He wore dark clothing, a hat, and sunglasses, and he kept both hands in his pockets. He looked suspicious enough that a platform employee scribbled a note on a piece of paper and gave it to the teller at the end of the line, whispering, "Pass it down." The note said, "Watch out. I think this guy's going to rob us." The note was read by each teller and passed on before the man was finally called from the customer line by the next available teller. When he approached the counter, he pulled a holdup note from his pocket and robbed the teller before escaping across a busy intersection.

This incident characterized the typical actions of employees before specialized lobby management training. After the training, employees began to feel comfortable noticing and approaching customers in their lobbies. Timed to coincide with a company-wide program on customer service orientation, the lobby management training reinforced the concept that each associate is his or her own first level of security. The associates were empowered to be proactive, aggressive, and observant.

The Outcome

After the lobby management training was given, incident reports flowed into the corporate security office describing suspicious persons who were deterred after being greeted and approached by an observant staff member. Corporate security was able to match descriptions of persons from different branches to determine that a particular individual indeed seemed to be “probing” branches for the purpose of robbing one. A month later, the suspect was captured after robbing a competing bank. Corporate security compiled numerous other examples of criminals robbing competing banks minutes after being approached in one of our banks.

Robbery reduction involves many factors, including prevention or apprehension equipment, security officers, and training. The benefits of a well-rounded program appear to be greatly enhanced when the program involves extensive hands-on contact and training from the security department.

The local robbery rate has dropped 86 percent in one year. Lobby management training, greeter stations near bank entrances, and diligent reporting of suspicious persons are now standard in the region.

J. D. Decker
Vice President, Corporate Security

Bank of America
1130 K St.
Sacramento, CA 95814

(916) 321-4905
joe.decker@bankofamerica.com

Industry	Employees	Yearly Revenue
Aviation	1,700	$500 million

Maintaining Worker's Compensation Insurance Coverage

The Problem

Chicago's Department of Aviation manages two airports: O'Hare International (the world's busiest airport) and Midway Airport. The department's employees consist of administrative personnel and operational staff. Most of the worker's compensation (injury-related) claims come from the operational personnel, including security staff, airfield operations staff, motor truck drivers, skilled trade workers, laborers, operating engineers, and custodians.

The cost of worker's compensation insurance escalated in recent years, largely in response to the terrorist attacks of September 11, 2001. The department faced a problem: namely, maintaining quality worker's compensation insurance coverage.

The Response

The response included a complete reassessment of procedures, including administrative controls, safety-related training, and procurement and maintenance of personal protective equipment. Now, work-related injuries must be reported within 24 hours, and the onus for such reporting falls on the injured employee's immediate supervisor. All accident reports are forwarded to the department's safety section and personnel section. The safety section reviews and electronically catalogs the incidents. Accident trends can more readily be detected, and appropriate responses, such as procuring personal protective equipment or conducting safety training, can be directed where needed. Similarly, the personnel section maintains a repository of information and works with the private claims management organization retained by the department to assist in the administration of the worker's compensation program. The personnel section focuses on lost time, including duty disabilities, related medical treatments, and required modified duty. In short, administration of the worker's compensation program is a joint effort by the safety and personnel sections and outside consultants.

The Outcome

Various safety training programs initiated by the department have led to measurable results with indirect financial impact. For example, in 1997, the department and the National Safety Council developed an ongoing defensive drivers program, which is unique to O'Hare Airport. The program has certified more than 300 special police officers and motor truck drivers responsible for airfield security, maintenance, escort activities, and snow removal in this complex and potentially dangerous environment. In addition, the personnel section now analyzes employees with repeat workplace injuries. Such analysis helps direct training and in some instances points to possible fraud. All these programs were recently reviewed for the most recent insurance underwriting.

Direct financial impact can be seen in insurance figures. For example, in 2000 there were 305 employee injury claims; 237 were medical only, and 68 were indemnity claims. The total amount paid that year for worker's compensation claims was $1,625,488.50. In 2002, there were 275 injury claims, 215 of which were medical only, and 60 were indemnity claims. The 2002 payout was

$1,324,660.46. Some cases remain open, but there has been a clear reduction in overall injury claims and associated costs.

As a result of these initiatives, the department has been successful in renewing worker’s compensation coverage with a reputable insurance carrier in a market noted for escalating costs.

Edward R. Le Fevour
Assistant to the Commissioner
for Safety and Security

City of Chicago
Department of Aviation

(773) 686-6490
av00279@ohare.com

SECURITY MANAGEMENT

Industry	Employees	Yearly Revenue
Utility	1,000+	$1 billion+

24-Hour Staffing for Emergencies

The Problem

Beginning on September 11, 2001, a large utility activated its emergency operations center (EOC) with an emergency response duty officer on a daily basis, 365 days a year. While the organization eventually scaled back from 24-hour EOC staffing, it kept a duty officer in the EOC during core business hours, even on holidays and weekends, for an extended duration. Each day, the EOC duty officer would check facility and infrastructure condition, report the findings, and note any security incident that may have taken place in the preceding 24 hours. The EOC would also notify on-call security representatives, who dealt with any security problems. Eventually, fiscal pressures, including significant overtime charges, required finding and implementing a different approach. The dilemma was how to do things differently without any loss in after-hours coverage.

The Response

Managers from security, emergency management, and operations brainstormed to arrive at a solution. They came up with the Protective Triad, consisting of an EOC duty officer, an on-call security professional, and a utility operator. The EOC remain in place, with the two most senior EOC duty officers rotating responsibility for monitoring status and issuing reports, but only during business days during Homeland Security Alert Condition Yellow and below. The EOC duty officers use cellular telephones and laptop computers with wireless Internet connections to communicate with 24-hour operations staff at various locations in the event of telephone outages. The EOC duty officer who is not on duty is on standby. In addition to their own, individually assigned pagers, the two EOC officers share a single pager dedicated to EOC business. In a parallel function, a security professional is on call 24 hours a day to manage the security response to any incident. Operators at the control center co-located with the EOC field EOC calls when the EOC is unstaffed. Those operator can quickly notify the EOC duty officer via the EOC pager.

The Outcome

Ultimately, the utility instituted three-way consultation on any unusual incident. When a suspicious incident occurs after business hours, representatives of these three disciplines quickly confer and invariably follow a better course of action than any single person would have chosen alone. For example, while the security professional calls law enforcement or sends a security patrol to a remote site with a problem, the EOC duty officer makes appropriate internal notifications, and the operator works to minimize potential damage or disruption to the system. As a result, major overtime expenditures have been significantly reduced and the quality of response has improved.

Nick Catrantzos, CPP
Security and Emergency Manager

The Metropolitan Water District of Southern California
700 N. Alameda St.
Los Angeles, CA 90012

(213) 217-7134
ncatrantzos@mwdh2o.com

Industry	Employees	Yearly Revenue
Retail	62,000	$8.2 billion

Achieving Return on Investment from Crime Analysis

The Problem

In late 2001, a retail chain implemented a program to assess the risk at each of the company's stores so appropriate security measures and levels could be deployed. The company's security team decided that the most accurate way to assess risk was to use its internal security reports and actual crime data from each police department where company stores are located. Because the company's stores are often the anchor stores in strip centers, many crimes were reported from the stores that did not actually occur there. To resolve the issue of over-reported crime, the security team had to find a method that would differentiate between two types of crimes: those that occurred at the store and those that were simply reported from the store.

The Response

In 2002, the security team began using a crime analysis software application. The software contains a crime database for each of the company's stores and verifies the nature and occurrence location of each serious crime, using police offense reports. The database includes the time, date, and specific nature of each crime. The database also reflects where violent crimes occurred on the property and identifies the victim. That information enables the security team to determine (1) whether a store is high, medium, or low risk, and (2) who is being targeted (customers or the store itself). Armed with store-specific data and the analytical tools in the software, the security team deployed appropriate security measures to reduce the risk at each store specifically.

The Outcome

By the end of 2002, a sizable return on investment was realized. An annual savings or cost avoidance of $9.2 million, 41 percent of the security budget, was gained in the first year since implementation of the new program. This savings reflects a number of changes to the security program, but the main change was the deployment of security personnel during higher-risk times. Before the use of the program, security personnel were used haphazardly, with no regard for actual risk levels. By deploying personnel only during peak risk times, the company saved over $9 million. It expects to retain a similar savings level in the years to come.

There is another category of cost avoidance that cannot yet be measured. That category consists of reduced crime and avoidance of security litigation—two benefits that the security team believes will accrue in the future. Over time, the company will build up enough data pertaining to settlements and judgments to determine if that hypothesis is correct.

With the software application, the security team is now able to select and implement appropriate security measures and justify its budget by allocating security resources based on empirical crime data. The savings to the company's bottom line has made the security department a favorite with upper management, which now allows the team the flexibility to experiment with other security technologies.

Karim H. Vellani, CPP
Security Consultant

Threat Analysis Group, LLC
P.O. Box 16640
Sugar Land, TX 77496

(281) 494-1515
kv@threatanalysis.com

Industry	Employees	Yearly Revenue
Contract Security	695	$21,649,054

Boosting Performance and Morale

The Problem

Contract security managers have the task of providing security officers with administrative support to help them carry out their duties effectively and in line with policies and procedures. Maintaining officer morale at a high level is an effective means of ensuring good performance.

Security managers can use many tools to boost officer morale. A contract security firm called Security Consultants Group (SCG) was awarded a federal government contract to provide security officers in Texas and Oklahoma. The previous contractor had filed for bankruptcy, leaving most of the 250 security officers without pay for the preceding six weeks of work. Upon accepting the contract, SCG inherited a workforce that was frustrated, even angry. Each officer's case was unique, but the overall condition was low morale. Once the officers' financial concerns were rectified, the company set forth to boost morale.

The Response

- *Scheduling.* A system of fair scheduling was developed so security officers would know well in advance what their work schedule would be. That way, they could plan their personal lives, including vacations and other family activities, accordingly. Performance and seniority are the primary factors that determine what schedule an officer receives. Better performance and more seniority equals a more favorable schedule.

- *Fair Discipline.* The contract security firm implemented a progressive disciplinary policy to reduce the discretion available to supervisors. This process ensures that officers are aware of what the punishment is before committing an infraction, while limiting inequities by supervisors.

- *Recognition.* The firm instituted an "officer of the quarter" program, which recognizes officers who have exceeded written expectations. The program awards one officer from each contract with a certificate of accomplishment, a financial award, and recognition in the company newsletter.

The Outcome

Using the techniques listed above, the contract security firm succeeded in boosting morale among its officers. As a result, the company has been able to retain good officers and decrease turnover and associated costs. At a cost of approximately $3,500 per replacement officer, a reduction in turnover provides an opportunity to add to the bottom line.

Karim H. Vellani, CPP	Threat Analysis Group, LLC	(281) 494-1515
Security Consultant	P.O. Box 16640	kv@threatanalysis.com
	Sugar Land, TX 77496	

Industry	Employees	Yearly Revenue
Healthcare	500	$40,153,624

Boosting Standards Compliance

The Problem

The Safety and Security Department at a psychiatric hospital for the criminally insane was not meeting legal and professional documentation requirements related to patient seclusion and restraint. Seclusion and restraint is a very high-risk procedure, used as a last resort to manage patients' behavior. Audit reports showed that the department was deficient in terms of practices and documentation. In many instances, compliance was below 50 percent.

Adding to the challenge, the department was experiencing major changes. Many forensic security supervisors were taking advantage of early retirement. The replacements hired by the department were inexperienced with documentation requirements. Also, the seclusion and restraint policies, procedures, and forms were constantly being modified to keep up with changing standards.

The Safety and Security Department is a mission-critical, high-visibility service department at the hospital. It operates around the clock with stationary and roving patrols and employs 46 forensic security supervisors and 200 forensic security aides.

The Response

The deputy director of safety and security first took corrective action of a punitive nature. Staff members received progressive discipline for failing to document seclusion and restraint. However, that approach did not significantly reduce deficiencies.

Next, the FADE model was put into action:

- *Focus.* A special meeting was initiated to focus on concerns, based on audits, that comprehensive oversight of seclusion and restraint was lacking.

- *Analyze.* Existing seclusion and restraint policies were analyzed for compliance with the Mental Health Code, administrative rules, and standards of the Joint Commission on Accreditation of Healthcare Organizations.

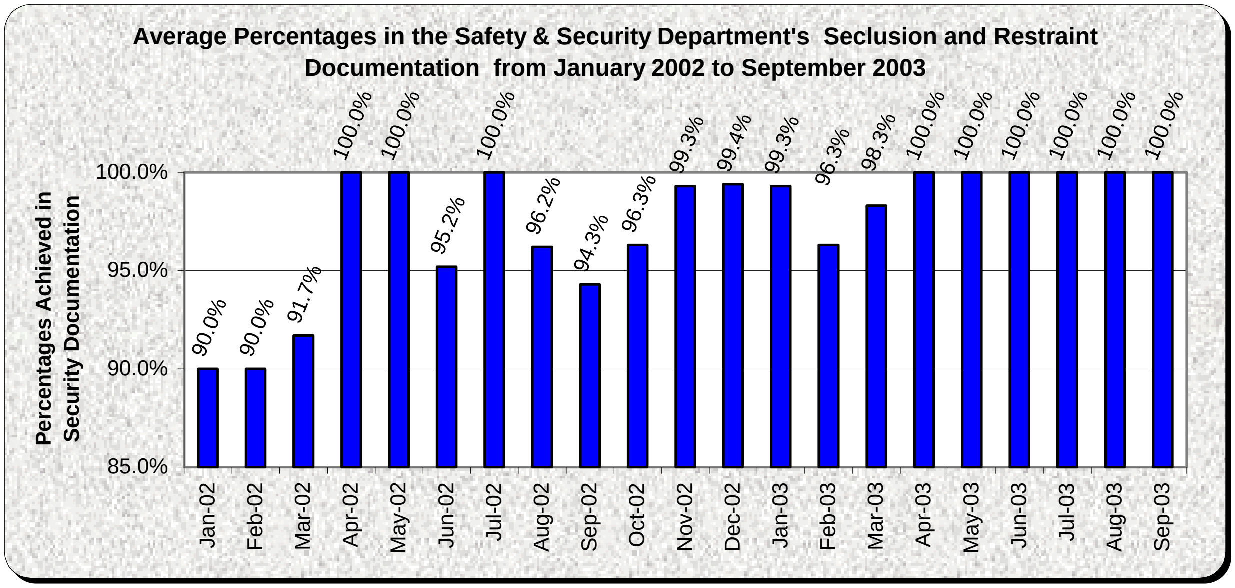
- *Develop.* A multi-departmental workgroup met to develop a form for improving documentation of seclusion and restraint incidents.

- *Execute.* The workgroup revised policies and procedures and developed a new audit form.

Security staff used the new form to document who performed the security checks for seclusion or restraint episodes. This change helped staff take ownership of and pride in their work. For staff who made repeated errors, the department provided additional training. In addition, security unit supervisors were required to check the forensic security aides' entries at the end of each shift. A goal of 95 percent accuracy in seclusion and restraint documentation was set.

The Outcome

Errors in seclusion and restraint reporting were greatly reduced. The Safety and Security Department exceeded its goal of 95 percent accuracy, based on an average of 300 documentation requirements for security staff per audit. (See graph.) The new goal, already attained over the last six audits, is 100 percent accuracy.


Average Percentages in the Safety & Security Department's Seclusion and Restraint Documentation from January 2002 to September 2003

Robert R. Greenwood
Deputy Director of Safety and Security

Center for Forensic Psychiatry
P.O. Box 2060
Ann Arbor, Michigan 48106

(734) 429-2531 Ext. 320
greenwoodr@michigan.gov

Industry	Employees	Yearly Revenue
Retail	1,200	$85 million

Cash Deposits in a Growing Company

The Problem

Deposits from company's 200 retail stores were to be made nightly or the following morning. The accounting group was supposed to reconcile each location's account to confirm that deposits were made. However, the accounting group did not see that task as a priority and therefore would never challenge locations if deposits were not made in a timely manner. If the location did not send in its paperwork detailing daily transactions, the accounting group would not find out about missing deposits until later when the accounts were reconciled.

This laxity was known by employees at many of the locations. When some employees ran into financial difficulties, they took the deposits. One manager who was caught taking money explained that she had originally planned to pay it back. However, she had never been challenged about the deposits, so she continued to take money. Her theft over an extended period to support a gambling addiction resulted in a loss of $35,000.

The Response

An investigation revealed weaknesses in the cash-to-bank program and back office audit routines. An additional auditor was hired. New procedures, including electronic reporting, were introduced.

The Outcome

Initially, there were no further losses of cash deposits. However, as additional stores were introduced into the chain, the problem surfaced again. Store employees were prosecuted. An additional auditor was hired.

The lesson learned was that, as the chain grew, the back office audit routines had to be adjusted to accommodate the additional workload. Adjustments included upgraded technology and additional personnel.

Brian A. Evans, CPP
Managing Director

The Evans Consulting Group
237 Kingston Row
Winnipeg, MB R2M OT1

(204) 233-8267
baevans@mts.net

Industry	Employees	Yearly Revenue
Insurance	30,000 (worldwide)	$117 billion

Compressing Security Officer Schedules

The Problem

At a large insurance organization, a security officer scheduling system based on end-to-end eight-hour shifts presented several problems. If an officer did not report to work, another officer had to be brought in for eight hours of overtime as a replacement. The unacceptable alternative was to leave the vacancy unfilled for the day. In addition, the eight-hour scenario did not allow for flexibility in the event of an emergency or special event. Shifts could not be adjusted to increase the number of officers on-site at a given time. Thus, eight-hour shifts were crimping the company's flexibility and requiring substantial amounts of overtime to be paid.

The Response

In an effort to boost officer coverage, reduce crime, and provide a benefit to improve officer retention, the company relinquished the schedule of five eight-hour shifts for security officers and switched to four 10-hour shifts. The new shift times are as follows:

- First shift: 6 a.m. to 4 p.m.
- Second shift: 11 a.m. to 9 p.m.
- Third shift: 9 p.m. to 7 a.m.

The one-hour overlap between 6 a.m. and 7 a.m. allows for extra officers during a peak service time. The five-hour overlap between 11 a.m. and 4 p.m. puts more officers on-site when most of the employees are in the building and the crime risk is higher. The overlap also allows for training to be done on shift without overtime.

Further, the second shift start time can be moved back and forth to accommodate special events or emergencies without the need for overtime. If an officer misses duty, it is only necessary to replace the officer's hours for the period before or after the overlap periods instead of for the entire shift.

The Outcome

As a result of the scheduling change, overtime has nearly been eliminated, saving $200,000 in the first year. The employees note a greater presence of security officers and have asked if the security department doubled its personnel allotment. Overall, crimes are down 11 percent, and service level audits have resulted in perfect scores. Training time has greatly increased without the use of overtime. New tasks and posts have been developed to ensure officers are productive in the overlap periods. The result is a higher level of service to the employee population.

A side benefit has been officer retention. Each officer has three consecutive days off every week. Officers see the new schedule as a significant benefit in their personal lives.

Jay C. Beighley, CFE, CPP
Director, Enterprise Security

Nationwide Insurance Enterprise
1 Nationwide Plaza
Columbus, OH 43215

(614) 249-7103
beighlj@nationwide.com

Industry	Employees	Yearly Revenue
Insurance and Financial Services	80,000	$5.5 billion

Establishing a Global Physical Security Policy with Best Practices and Minimum Requirements

The Problem

American International Group (AIG), an insurance and financial services organization active in approximately 130 countries and jurisdictions, operates in both owned and leased environments at over 2,000 individual office locations. Each office presents unique physical security concerns. After the terrorist attacks of September 11, 2001, AIG's chief security officer was concerned that standardized operational and physical security procedures were not defined and that a policy defining an acceptable baseline of security was needed.

The Response

In fall 2002, AIG began studying its embedded base of security in order to better understand the company's broad security stance. The Corporate Security Department developed a substantive physical security survey, addressing such topics as access control hardware, guard programs, landlord security programs, and perimeter security. The document was disseminated electronically to all company sites worldwide. Executive buy-in and support helped the department obtain a thorough and timely response to the survey. Upon capturing the data, AIG Corporate Security observed inconsistencies in security resources. Using categories including head count, profit center status, and local threat ratings, the department ranked sites according to their need for immediate attention and physical security upgrades.

In addition, the survey findings were compared to industry best practices and minimum requirements. For example, AIG space in a high-threat offshore environment might require vehicular road-blockers and armed guards to meet best practices, though when all criteria were assessed, the minimum requirements of controlled parking and electronic access control were deemed acceptable. Corporate Security authored a complete policy reflecting best practices and minimum requirements. The policy includes subsections dealing with the specific measures to be considered in protecting shared lobbies, garages, and core interior areas such as telephone closets and computer rooms.

The Outcome

To date, Corporate Security has received completed physical security surveys for more than 700 AIG locations. The Best Practices and Minimum Requirements Policy has been posted on the company's intranet and disseminated to appropriate business leaders. In addition, Corporate Security is ensuring that the new physical security policy serves as a tool for end users, the administration group, and realty professionals within the company.

By using the data captured in the survey, and by rolling out the policy, Corporate Security has enhanced access applications, guard deployment, and operational security procedures so as to mitigate risks to AIG people and property. The migration to physical security standards, such as deployment of a standardized access card and access system technology, also results in cost advantages. For example, in the first half of 2003, the company realized a 50 percent savings in card procurement expenditures compared the first half of 2002.

Nicholas A. Smith, Jr., CPP
Director, Global Physical Security

American International Group
70 Pine St., Lobby
New York, NY 10270

(212) 770-7018
nicholas.smith@aig.com

Industry	Employees	Yearly Revenue
Healthcare	1,800	$200 million

Improving Internal Customer Satisfaction

The Problem

Over a period of several years, Security Department employees at a hospital were becoming increasingly unproductive. The department lacked firm, fair, and consistent leadership; some personnel were unqualified; and, on the whole, the department seemed reluctant to take on new duties and responsibilities. This combination resulted in a lack of teamwork among the officers and gave other hospital employees little confidence in the department's capabilities.

The depth of the problem became evident in the results of the hospital's employee opinion surveys, which were administered every three years by an independent consulting firm. The results of the 1996 survey showed that among the Security Department staff there was a significant decline in the category called "proud to work for the organization." The average Security Department score was 2.6, while the average score across all hospital departments was 2.3. (Note: For this type of survey, the lower the number, the better or more positive the response). The results of the 1999 survey showed a further decline. The Security Department's average worsened to 3.9, while the average department's response improved to 2.1.

The Response

In response, the hospital took the following steps:

- The hospital retained the services of a security consulting firm to review all security operations.

- A new, experienced security director was hired.

- A new mission and vision statement was created for the department, job descriptions were revised, and the name of the department was changed to Security & Safety Services.

- Employees of the department were referred to as "team members."

- New duties and responsibilities were added. For example, the department petitioned for and received approval for all uniformed officers to obtain state-issued "Special Conservator of the Peace" status.

- To go along with the new responsibilities and duties, team members were given a commensurate pay increase.

- A department-specific survey of the needs and desires of team members was conducted, and the results were shared with all team members.

- Suggestions made by team members to improve operations were quickly implemented.

- Formal recognition efforts were developed. For example, a large award plaque was obtained, and when individual team members performed above and beyond the normal call of duty, their names were placed on it as a mark of honor. Also, at each monthly department meeting, time was allotted to formally recognize the work of team members.

- Outdated practices were discarded.

- A formal training program was developed.

The Outcome

The results of the 2002 employee opinion survey showed a dramatic improvement in all security department scores. The new score for the category "proud to work for the organization" was 1.6 (a significant improvement from the previous score of 3.9). Perhaps even more telling, for the first time in six years the department's score surpassed the average score for all hospital departments together (1.8).

In addition to the improvement in the survey results, the department began to receive compliments from other hospital employees, stating that they too noted and appreciated the change in the level of service provided by all security and safety personnel. The challenge now is not merely to maintain this level of confidence, but to use the knowledge and experience of all team members to further improve the department's ability to provide the best possible protection services to everyone.

Paul D. Lockwood, CPP
Assistant Director of Facilities
Management/Security &
Safety

Rockingham Memorial Hospital
235 Cantrell Ave.
Harrisonburg VA, 22801

(540) 564-5493
PLockwoo@rhcc.com

Industry	Employees	Yearly Revenue
Healthcare	6,000	unspecified

In-House Training by Security Staff

The Problem

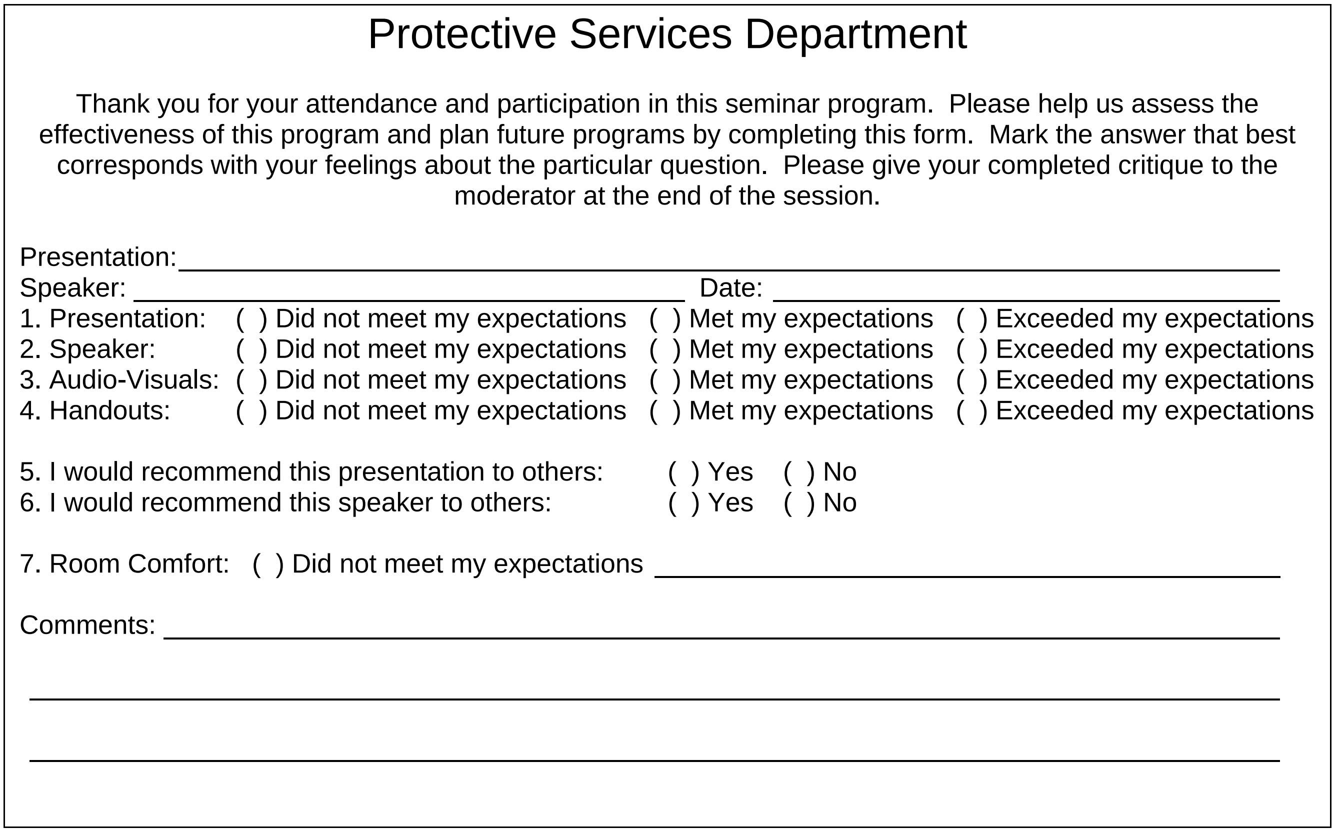
Training and retraining employees is an ongoing challenge for many institutions. It is a particular challenge for organizations that face an elevated risk of robbery because they contain credit unions, cafeterias, gift shops, or other such targets. Hospitals especially fit that description.

For Cincinnati Children's Hospital Medical Center, frequent training on robbery behavior is needed, as new employees are hired throughout the year. Outside sources of training are numerous, yet they tend to offer their courses only at specific times and dates, which are not always convenient for hospital staff. Moreover, the required training and retraining can be very costly, and outside providers are not as familiar with the hospital as in-house security staffers are.

The Response

The hospital's Protective Services Department provides robbery behavior training with its own staff. The many available books and manuals, plus the vast world of Internet information, combined with the department's years of experience, were used to form an in-house training program. The training is provided to new employees, as well as those with years of service. Students are taught what to do and what not to do in the event of a robbery. In particular, they are taught how to react, how not to react, what to look for, what not to touch, what not to say, what body language to use, and so on.

This training may be presented at any time and place requested by the employer or employees. The Protective Service Department documents the training sessions by using sign-in sheets for attendees. The quality of instruction is maintained with the use of a simple critique sheet (see illustration), which enables training participants to provide feedback at the end of the presentation.



Protective Services Department

Thank you for your attendance and participation in this seminar program. Please help us assess the effectiveness of this program and plan future programs by completing this form. Mark the answer that best corresponds with your feelings about the particular question. Please give your completed critique to the moderator at the end of the session.

Presentation:____

Speaker: ______________________________ Date: ____________________

1. Presentation: ( ) Did not meet my expectations ( ) Met my expectations ( ) Exceeded my expectations
2. Speaker: ( ) Did not meet my expectations ( ) Met my expectations ( ) Exceeded my expectations
3. Audio-Visuals: ( ) Did not meet my expectations ( ) Met my expectations ( ) Exceeded my expectations
4. Handouts: ( ) Did not meet my expectations ( ) Met my expectations ( ) Exceeded my expectations

5. I would recommend this presentation to others: ( ) Yes ( ) No
6. I would recommend this speaker to others: ( ) Yes ( ) No

7. Room Comfort: ( ) Did not meet my expectations ________________________

Comments: ____

____

____

The Outcome

The Department of Protective Services is able to provide this type of training to the staff on an ongoing basis. The training is cost-effective and keeps the staff well informed on what to do during a robbery. Further, hospital staff feel at ease receiving training from their own security department staff. The training is tailored to their particular working environment in a way that outside trainers could never match.

Philip K. Keller
Manager, Protective Services
Department

Cincinnati Children's Hospital
Medical Center
3333 Burnet Ave.
Cincinnati, OH 45229

Industry	Employees	Yearly Revenue
Contract Security	undisclosed	undisclosed

Key Performance Indicators for Contract Security Programs

The Problem

A major security firm provides contract security services to Fortune 500 firms throughout the United States. Many of the firm's clients—especially their strategic sourcing departments—are accustomed to gauging contract effectiveness through quantitative measurement. Therefore, the security firm must show the return on investment (ROI) that its services provide, especially for larger, multi-site contracts. The problem, then, is to develop quantitative measures that demonstrate ROI.

The Response

The security firm worked with several clients to develop key performance indicators (KPIs) that tie into the ROI or the specific contribution that clients want their contract security program to provide. As client needs, visions, missions, and cultures vary, the KPIs for pharmaceutical clients are different from those for petrochemical producers or financial services firms. However, core KPIs—such as safety, turnover, training proficiency, management response, alarm and incident response, report writing, and customer service—apply to all types of facilities and security programs.

The security firm attempted to develop KPIs that are quantitative and easily measurable. Customer service is very important to clients, but it is difficult to measure quantitatively. The firm developed an easy-to-complete e-mail survey that enabled client employees to report their feelings about the effectiveness and value provided by the contract security program. The survey inquires about the customer service skills of the security firm's employees. The survey uses numerical ratings to facilitate quantitative measurement. Now in use in several large, multi-site client programs, the survey provides excellent feedback. At one client site, over the period of a quarter, the security firm noticed a decline in KPI for customer service. The ratings dropped from 4 ("excellent") to 3 ("acceptable"). The security firm provided its officers with refresher customer service training from an outside resource. In following quarters, the customer service KPI rose back up to the former level of "excellent."

After developing KPIs with a client, the security firm then measures results on a periodic basis, usually quarterly, and meets with client contacts, typically both security and strategic sourcing management, to review data. During these meetings, the security firm identifies strengths and determines whether there are "best practices" that should be communicated to other client sites. At the same time, the security firm attempts to discover the root causes of weaknesses, formalize corrective actions, and, during subsequent meetings, track the results of corrective actions taken. When a weakness is corrected, the security firm may develop "lessons learned" that will be transmitted to other facilities. When the security firm noted a sudden lowering of KPI marks for safety at a client site because of a rise in vehicle accidents over a month, it determined driving requirements had been significantly increased, especially during hours of darkness. The security firm instituted increased driver training, with special emphasis on night operations, and the KPI marks for safety quickly returned to their former level of "outstanding" at the site. As vehicle operations requirements at this client's other facilities serviced by the security firm had similarly changed, a "lessons learned" driver training revision was generated for all sites.

In addition, quarterly KPI meetings address the relevance of the performance measurements being used and consider what changes, if any, should be made to them.

The Outcome

Using measurable KPIs has helped demonstrate the value of safe, quality-oriented contract security programs to strategic sourcing and financial departments within client organizations. Performance measurements have helped clients show that security programs can significantly contribute to providing safe and productive work environments for their firms' employees. In some contracts, a portion of the security firm's profit is tied to performance. Incentive bonuses may be paid for hitting "stretch goals." Portions of those bonuses are shared among security staff, emphasizing the importance of their contributions to both the client's and the security firm's visions and missions.

Richard E. Moulton, CPP, PSP
4 Swedes Lane
Moorestown, NJ 08057
(267) 738-4954
pmmoulton@earthlink.net

Industry	Employees	Yearly Revenue
Mining	1,600	$200,000,000

Large Turnover of Security Personnel

The Problem

For two years, the company had experienced an annual turnover rate of approximately 25 percent within the Security Department. The majority of the personnel left to obtain the higher wages being offered by another organization. The turnover was damaging to the morale of the security officers who remained with the company.

The Response

The company was unable to exceed, let alone meet, the wages being offered at the other organization. As an alternative means of keeping staff, the company initiated several programs designed to curb the loss of manpower and increase morale, loyalty, and productivity.

New training programs were started in the basic course and ongoing training courses. Outside instructors were brought in to teach courses. Certificates were given to all who completed a course. This upgrade of training gave the officers a better sense of their worth to the company

A Security Department membership to a sports complex/fitness center was obtained. That benefit showed the officers that the company cared about them and would do what it could for them.

Sports tournaments (volleyball, soccer, and basketball) were held on a random basis. Those activities also proved to be a morale booster.

The Outcome

Since the initiation of these programs, the company's attrition rate has dropped to approximately 5 percent. In addition, there have been fewer reports of theft, and officers have provided a greater number of written suggestions on how to enhance security.

Robert F. Marcelain, CPP	Kumtor Operating Company	996 612 600707
Corporate Security Manager	24 Ibraimov St.	robert_Marcelain@kumtor.com
	Bishkek, Kyrgyzstan 720031	

Industry	Employees	Yearly Revenue
Government/Military	15,000+	n/a

Performance Management in Army Antiterrorism/Force Protection Program Activities

The Problem

Like many other military organizations in the aftermath of the September 11, 2001, terrorist attacks, the United States Army Communications-Electronics Command (CECOM) found itself scrambling to implement controls and preventive measures to protect its people, facilities, and mission critical operations around the globe. It was not long before the prioritization of project funding and equipment procurement became complex and random; efforts to improve the more obvious problem areas became commingled with more complicated projects; and the line between short- and long-range planning was blurred. As a result, CECOM sought opportunities to improve its Antiterrorism/Force Protection (AT/FP) Program. It was learned that the program lacked performance metrics, quality standards, and other systems and procedures that drive continuous process improvement.

The Response

In spring 2002, CECOM installations began applying measures to enhance protection efforts. For example, they started tracking vehicle throughput at depot access points where individual identification and vehicle search activities were significantly delaying entry and disrupting business operations. The collected data were used to determine resource needs during fluctuating threat levels (increased or decreased), with their requirement for increased or decreased protective measures. Headquarters committed to build in overarching continuous process improvement throughout the command. A policy analysis was conducted to identify the desired outcomes (not simply the procedural requirements) of the AT/FP Program.

Ultimately, an evaluation process was designed to address each of the critical tasks and subtasks across the spectrum of disciplines beneath the AT/FP umbrella, such as information system assurance, vulnerability exposure, law enforcement and physical security activities, and weapons of mass destruction consequence management planning and operations. The activities are assigned a weighted score that culminates in an overall score, thereby providing both an in-depth analysis and a snapshot summary of the AT/FP posture for major activities, population centers, and subordinate organizations within CECOM.

Each month, the activities are reviewed to identify deficiencies, root contributors, and successes across the enterprise. Process improvement opportunities are discussed and implemented by the functional experts serving on the Command AT/FP Working Group. A “project action register” is used to communicate team activities and support collaboration. The CECOM intranet-based knowledge center portal serves as a conduit for information circulation across the command.

To track the effectiveness of the AT/FP awareness training provided to all employees, contractors, military service members, and their families traveling or assigned overseas, a customer value survey process was implemented. The survey identifies not only the value perceived by the traveler, but also the “freshness and relevancy” of the threat advisory and related intelligence being provided. This value survey has also been converted to a metric with results reported monthly.

The Outcome

In the first six months of 2003, CECOM has achieved a nearly 16 percent increase in AT/FP process improvements across the enterprise. Another result of the performance management process is the easy conversion into a balanced scorecard reporting process, now joining the key CECOM business lines and major activities. The Army-wide effort to implement a Strategic Readiness Report (essentially a balanced scorecard) is challenging most AT/FP practitioners; CECOM on the other hand, simply passes existing, validated data into the headquarters system. The composite score on the AT/FP Customer Value Survey has climbed to 4.30 on a scale of 1 to 5, with 4 reflecting “time well spent” and 5.0 reflecting “time very well spent.”

In July 2003, the Army Materiel Command (AMC), with over 150,000 personnel, named CECOM as the only one of six AMC major subordinate commands to have achieved an assessed performance level exceeding 94 percent across all functional areas within the AT/FP arena.

Robert A. Young, CPP
Antiterrorism/Force Protection
Program Officer

US Army Communications-
Electronics Command
AMSEL-OC, Bldg 1209,
Room G13
Fort Monmouth, NJ 07703

(732) 532-8399 x0332
Robert.a.young1@us.army.mil

Industry	Employees	Yearly Revenue
Retail	2,000	$100 million

Refund Fraud

The Problem

At a retail chain, managers had been instructed to review all returns to ensure customer satisfaction and the legitimacy of the return. Reasons and conditions were to be recorded, including whether the customer purchased something else, manufacturing problems were known, and the returned product was usable. Managers were supposed to review each refund and sign off on it. Because managers were sometimes away from the stores (due to days off, lunch hours, or other reasons), it was not always feasible for them to review returns immediately. Therefore, company policy was amended to state that managers must review all refunds at the end of each day or else the next day when they came in to work.

One manager claimed the policy did not make sense and that following it would take him away from many other priorities that required his attention. He declined to follow the policy.

An employee who knew the manager would not review refunds created a fraudulent refund scheme. According to the employee, the fraud began at $50 per week. By the third month it had reached $250 per week, and by the sixth month, $400 per week. The scheme took seven months to uncover. Finally, the regional manager noticed the store’s high refunds and low margins. A review of refund history revealed the fraudulent activity.

The Response

The employee admitted the theft of cash—in excess of $5,000—and was criminally charged.

All sales managers are now required to review refunds immediately upon returning from coffee breaks, lunch breaks, and days off. Customers are contacted to ensure they are satisfied with the service. Regional managers audit the process as one of their audit reviews when visiting stores. All “no bill” or “no receipt” refunds must receive the approval of the regional manager, and the retail auditor verifies the process.

The Outcome

Refund fraud is not the only cause of stock shortage. Nevertheless, if left unchecked, it can result in substantial losses. Now, with the new refund procedures in place, refund fraud is all but eliminated and stock shortages remain under 1 percent.

Brian A. Evans, CPP	The Evans Consulting Group	(204) 233-8267
Managing Director	237 Kingston Row	baevans@mts.net
	Winnipeg, MB R2M OT1	

Industry	Employees	Yearly Revenue
Aerospace	3,000	$2.2 billion

Regulatory Compliance

The Problem

The company in this illustration manufactures solid-propellant rocket motors for military, space, and commercial launch vehicles. Export of the company's products, technologies, and services is controlled by the International Traffic in Arms Regulations (ITAR). Therefore, when dealing with foreign customers and vendors, the company often must obtain export licenses from the U.S. Department of State.

The licenses, especially "technical assistance agreements" and "manufacturing license agreements," are often complex documents with many limitations and provisos. When the corporate office for which the license was obtained does not understand the license, there is a serious potential for non-compliance, which can result in fines, debarment, and imprisonment of company officials.

The Response

First, the company developed a simple checklist that is completed for each new license. It identifies such items as type of license, category of material to be exported, and recipient of material. It also captures the name of the person or persons responsible for implementing the license and lists any limitations and provisos.

Second, an export-import control officer meets with the responsible person or persons to go over the license and checklist point by point. In that meeting, the participants resolve any issues that might come up. For example, they may contact other export-import control officers in the company, contact legal counsel, or turn to the corporate "empowered official" for resolution. Problem resolutions are documented and filed with the office copy of the license.

The Outcome

The measure of success is avoidance of non-compliance. It may be premature to determine whether the form and meeting are effective, as this approach has been in place for only six months. However, it appears that the form and the meeting are having the desired result. Both the persons responsible for implementing the license and the export-import control officer have a better understanding of what must be done to comply with the license. In the six months the form and meeting have been in use, there have been no non-compliance issues related to the licenses covered in this new approach. (The form is available by request to the author.)

Kenneth C. Freimuth, CPP
Security Manager/Export-Import Control Officer

ATK Thiokol Propulsion–Promontory
P.O. Box 707
Brigham City, UT 84302

(435) 863-3927
kenneth.freimuth@atk.com

Industry	Employees	Yearly Revenue
Retail	25,000	$1.5 billion

Retail Shrinkage Reduction: The Right Plan for Each Brand

The Problem

The marriage of two companies in 2001 to form one centrally managed, 25,000 associate, $1.5 billion company of three brands brought many changes, not the least of which was higher than normal shrinkage. The brands were optical retail, sunglass retail, and watch retail, each with unique problems. An aggressive plan of action was needed to bring high shrinkage stores under control, using one loss prevention department for implementation.

The Response

Optical retailing: Associates range from doctors to licensed opticians to unskilled frame stylists. Associates are career-minded and want to advance from within.

Stores were categorized as “high shrinkage” or “focus” stores if they had $5,000 or more in cost shrinkage from the last inventory period or if they had 75 or more eyeglass or sunglass frames missing. Loss prevention managers (LPMs) focused on those stores for operational audits. The detailed audits looked at inventory control, retail procedural controls, lab operations, physical security of the store, asset controls, and human resources. Before auditing a store, an LPM would use exception-based reporting to pull exception reports on cash refunds, voids, cash register paid-outs, no sales, and other variables. The reports helped direct the LPMs to problem areas and suggested investigations.

Audit scoring was performed, using weighted questions. Points earned were divided by total points possible. The score was conveyed to store management and field operations leadership as a performance standard for associates’ annual reviews. A score of 70-79 percent rates a 2 (meets most expectations); 80-89 percent rates a 3 (meets expectations); and 90-99 percent rates a 4 (exceeds expectations). A performance standard of 3 or higher is acceptable. The scoring helps store management and associates understand the need to take security controls seriously.

Each focus store had to complete an action plan to correct audit deficiencies and submit it to the supervising field executive. A store meeting was held to discuss results and give training on shrinkage reduction and shoplifting prevention. Stores with scores of 2 or lower were given follow-up audits 90 days later. Failure to take shrinkage control seriously could result in employment action up to and including termination.

LPMs also evaluated high shrinkage stores to determine if they were good candidates for electronic article surveillance, benefit denial tagging of products, public view camera systems, or locking display cabinets or towers. LPMs were empowered to make recommendations to field management executives, receive financial buy-in, and then order the equipment.

Sunglass and watch retail stores: Associates are younger, less loyal to the company (not career oriented but typically college bound or job hunting), often working alone and facing temptation from peers, family, and friends. Turnover is much higher in the kiosk and small in-line format of these stores.

Stores were designated as “high shrinkage” if they had shrinkage of $9,000 or lost more than 200 product units. LPMs would conduct half-day audits of those stores to uncover training needs. Training was given to store managers and regional managers, who could spend more time in the stores, reach more stores, and train more associates than the LPMs. The LPMs would also study exception-based reporting on cash refunds, manually entered credit cards, voids, gift card use, paid-outs, overrides, and other activities. Those reports gave LPMs insights into store practices and suggested investigations.

During focus audits, the LPMs verified counts of products against register readings of on-hand totals. In addition, refund call lists were verified by checking for returned product on the sales floor or on the damaged return list. After the audits, store managers had to provide action plans outlining what they would do to correct deficiencies. In addition, questionnaires about shrinkage causes were sent to associates to be filled out anonymously, if they so chose, and mailed (in pre-stamped, addressed envelopes) to the Loss Prevention Department in the corporate office.

In watch stores shrinkage was caused by battery replacement; batteries were replaced to please a customer and never removed form inventory by being entered into the point-of-sale system. A battery replacement log was instituted to track battery sales and counts. New battery vendors were found. Now, whenever a replacement battery is put in a new watch, the old battery goes into the new package and is returned to the vendor for credit.

The Outcome

Many synergies have been discovered, serving all brands in reducing shrinkage. The company now uses a single business abuse hotline to accept information on theft issues. All calls on the line are investigated. Another synergy is the use of a single information management system for recording internal investigations, external theft, and burglaries to help uncover trends and mutual problem areas. Yet another is the use of phone interviewing to reduce travel costs and increase the efficiency of the LPMs.

One of the best synergies is the use of a single exception reporting system, which captures information on each brand. It saves thousand of hours of research and gives complete and accurate information quickly. The central group of loss prevention analysts pulls data from the system, builds investigative cases, and feeds them to the loss prevention managers, who bring them to conclusion.

Results have been forthcoming each inventory period. From one inventory to the next, 67 percent of focus stores have dropped off the list, and they have not repeated. The last sunglass retail inventory showed a 59,000 unit reduction in shrinkage. The results clearly support the use of the new programs.

Alan F. Greggo CPP, CFE
Director, Loss Prevention

Luxottica Retail
4000 Luxottica Pl.
Mason, OH 45040

(513) 765-6289
Agreggo@Luxotticaretail.com

Industry	Employees	Yearly Revenue
Government	75	n/a

Staffing Optimization in a Unionized, Government Setting

The Problem

The Office of the Illinois Secretary of State is a branch of Illinois government, and the secretary is an elected official. One responsibility of the office is to provide security around the clock for the Illinois State Capitol complex, 26 buildings, and some 6,500 government workers and thousands of visitors daily. The security force consists of approximately 75 unionized officers.

State government budget deficiencies and early retirement programs reduced the security force by 28 officers during the period 1999-2003. The security force had been represented by a bargaining unit agreement since 1971, and shift schedules were established as 7:00 am-3:00 pm, 3:00 pm-11:00 pm, and 11:00 pm-7:00 am. Peak times of incidents (10:00 am-6:00 pm) coincided with the hours of government functions, and a straight shift rotation did not provide adequate security at peak times. Risk analysis indicated that the integrity of the overall security program was most at risk during events with a concentration of visitors and government business activity.

The Response

Negotiations with labor leaders in the bargaining unit led to the establishment of a noon-8:00 pm shift. This peak shift provided additional manpower to both the 7:00 am-3:00 pm shift and the 3:00 pm-11:00 pm shift. The staffing boost comes at a time of day when the majority of employees are in the Capitol Complex, the state legislature is in session, visitors are on-site, and most special events, rallies, and protests occur.

The Outcome

Optimum utilization of manpower during identified peak times provided additional integrity to the overall security program. Additional security staff were positioned and visible during the time of the greatest identified risks. The increase in visibility and availability of manpower improved response time to incidents. In addition, it appears that losses, parking lot incidents, and abuse of sick time have been reduced.

No additional costs were directly associated with the change in shifts. Oral surveys suggest that customer satisfaction has risen because of the increase in visible security presence.

Robert J. Orr, CPP Lieutenant Colonel–Special Operations	Office of the Secretary of State–Security Division P.O. Box 11175 Springfield, IL 62791	(217) 529-3260 mcgregorr@aol.com

Industry	Employees	Yearly Revenue
Insurance	30,000 (worldwide)	$117 billion

Threat Levels and Standards

The Problem

In an organization with 700 facilities around the world, it was difficult to ensure that each facility had the appropriate level of physical protection. Threat levels were identified not through an objective process but through anecdotal evidence and the personal feelings of on-site managers. The result was that protection levels were inconsistent and security costs and equipment specifications varied widely. In all likelihood, some sites were overprotected and others underprotected, but there was no way to know which was which.

The Response

To increase the uniformity and appropriateness of protection, the company established specific high, medium and low threat levels. Threat levels can be recommended based on the type of business activity, population of the facility, critical infrastructure on-site, local crime statistics, and other socioeconomic factors. These characteristics may indicate that a high-risk facility is one with a large population, critical business processes, valuable assets, and high local crime rate. Lower, varying levels of certain characteristics may indicate lower levels of threat and protection needs. The assessment is coupled with a physical security assessment of the site. The scores are then added together and compared to the score ranges assigned to each threat level.

In addition, physical security standards were established for each threat level. These standards specify required equipment, training, awareness, and security staffing. They are based on commonly accepted practices in the security industry.

Once the threat level for the site is established, the standards that have been designed to meet each threat level are applied. For example, a high-threat-level site is expected to have a closed-circuit television system (CCTV), electronic access control, an alarm system, and various polices, procedures, or training for employees. A medium-threat-level site may forgo the CCTV and exchange the electronic access control system for a system that uses less expensive technology. A low-threat-level site may have only an alarm system, relying mainly on protection provided by well-trained and aware employees.

The Outcome

The results of the program include the elimination of underprotection or overprotection of a given site and the attendant unnecessary risk or wasted expense. Facility services division staff and end users know clearly what level of protection to expect. Because the right level of protection is now applied to each site, computer theft resulting from burglaries has dropped 89 percent and robberies have been reduced to none.

Moreover, the bidding process for security installations is greatly streamlined, and security costs have declined. Because vendors now know how and in what locations equipment will be used, they can make quantity equipment purchases and cut their fees.

Jay C. Beighley, CFE, CPP
Director, Enterprise Security

Nationwide Insurance Enterprise
1 Nationwide Plaza
Columbus, OH 43215

(614) 249-7103
beighlj@nationwide.com

Industry	Employees	Yearly Revenue
Unspecified	Unknown	Unknown

Workforce Protection Planning

The Problem

X-Y is the fictitious name of a large industrial enterprise settled throughout Spain. The company is organized into a national headquarters and several local production and administrative centers that are accountable to it.

A general survey on protection and security responsibilities and practices, conducted by a specialized consulting firm in 2001, revealed a situation characterized by decentralization, lack of coordination, and even duplication of effort. The different protection functions were divided as follows:

- Physical security: accountable directly to the deputy general director
- Environmental protection: incorporated in Logistics Management
- Workplace safety and firefighting: under Logistics Management
- Personnel security: part of the Human Resources Department
- Medical emergency and biohazards: accountable to the human resources general director
- Computer and communications security: a function of the IT Department but with no specific personnel assigned
- Operations security: included in Production Department policies and procedures but with no specific personnel assigned

The situation was the perfect scenario for the waste of protection funds, constant conflicts of interest and competencies, and employee dissatisfaction, due to the patent perception that something was wrong with the protection and security function. X-Y management definitely felt uneasy about the situation.

The Response

The first step taken to solve the problem was the creation of a working group that would be able to reach a solution in a given period of time. The group was given one month to settle the “big picture” in a realistic way and identify a strategy to follow. The group included not only representatives of the main protection and security functions but also other employees and even customers.

At the deadline, the group selected a course of action. It included these measures:

- Adopt the term “workforce protection” as a whole to refer all the areas of the company related to protection and security. This was an attempt at conceptual integration.

- Create a global, transparent, and understandable workforce protection policy and distribute it to employees.

- Prepare a general workforce protection plan, a kind of steering plan, including the main aspects of the various specific protection and security plans.

- Create national and local workforce protection committees, which would coordinate efforts and procedures while optimizing economic resources. The committees’ main objective would be to foster interdepartmental communication.

- Identify several urgent, visible protection challenges that could be addressed to gain some quick results.

The Outcome

After implementing the actions listed above, impressive results were achieved:

- An immediate saving of protection and security funds was realized. Expenses were reduced by 10 percent during the first year.

- The meetings of the committees (national and local) and coordination activities effectively eliminated the problem of duplication and, consequently, waste of time and efforts. Mutual knowledge facilitated collaboration and understanding.

- Most employees who were surveyed (72 percent) indicated confidence in the new protection and security strategy, applauding the results of the actions taken. Now, greater emphasis is given to workforce protection functions.

Luis Hernandez Garcia, CPP
Major, Spanish Air Force

Acuartelamiento “El Rey”
Paseo del Pardo
El Pardo 28071 Madrid
Spain

00 34 91 7407010 ext. 7159
luahernan@yahoo.es