ITEBOOKS.DIRECTORY

INTELLIGENCE-BASED SECURITY IN PRIVATE INDUSTRY

ITEBOOKS.DIRECTORY

ITEBOOKS.DIRECTORY

INTELLIGENCE-BASED SECURITY IN PRIVATE INDUSTRY

Thomas A. Trier

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

ITEBOOKS.DIRECTORY

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

© 2015 by Taylor & Francis Group, LLC
CRC Press is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works
Version Date: 20150506

International Standard Book Number-13: 978-1-4987-2204-9 (eBook - PDF)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (http://www.copyright.com/) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

ITEBOOKS.DIRECTORY

CONTENTS

ITEBOOKS.DIRECTORY

ITEBOOKS.DIRECTORY

SECTION VII—Implementation: Case Studies

ITEBOOKS.DIRECTORY

ITEBOOKS.DIRECTORY

PREFACE

As I transitioned to private security from the Federal Bureau of Investigation (FBI), retiring after 25 years as a special agent, I found that many of the intelligence, analytical, and critical thinking skills that I had learned and utilized to dismantle criminal and terrorist organizations could be applied to the private sector. At my first civilian job as the security lead at an electrical transmission-only utility company, there was a problem with criminals who were cutting holes in the perimeter fencing and stealing copper grounding clamps and wire to sell as scrap. As I discussed this problem with security personnel, I discovered an attitude. The person responsible for asset protection in the Security Department told me, "Copper theft is like a lightning strike; you never know when and where it will happen." But, when I asked for security incident reports and police reports for the last 5 years to analyze for patterns, I was told the Security Department did not do security incident reports, and "it was too hard" to obtain police reports.

This was unacceptable; when I ordered another person to obtain the police reports, we found the police had made some arrests regarding the thefts. We started tracking these thieves and compiled an organizational chart of their contacts. Needless to say, utilizing the techniques I learned in the FBI, we reduced copper theft incidents from 29 in 2011 to 6 in 2013. The details of this initiative and others that led to the intelligence-based security posture program developed from these and similar efforts are presented in this book.

I was amazed at the disorganization in the security departments of other utility companies that I attempted to collaborate with and was actually surprised with the conflict that arose with them in developing some of these measures related to an intelligence-based security posture. Many of the security managers concentrated on having enough contract security guards on the property each day instead of what the security guards were doing and how they were doing it.

Even after we developed a list of "usual suspects" in the copper theft initiative, the other electrical utility companies we worked with were reluctant to participate and share information. One was "afraid to keep watch lists on citizens" even though I explained the offenders' list consisted of convicted felons, who might be citizens but had shown the

ITEBOOKS.DIRECTORY

capability to commit thefts from the substations under our care. This was a case of misunderstanding the principles of tracking known offenders and lack of experience in protecting a company from those who would do it harm. Also, adding to the reluctance to participate in the intelligence-based initiatives was the amount of work involved to set up an intelligence program. This is not easy. It can be beneficial once implemented, but the "climb" to the top of the mountain is definitely a difficult one.

This book is designed to be informational, allowing readers to understand the use of the intelligence-based security posture. It is meant to answer the following questions: What are the differences between a threat assessment, a vulnerability assessment, and a risk assessment? Do you know the difference between the intelligence-based security posture, designed to reduce risk to security, and business intelligence, which is designed to gain a competitive edge on the company's competition? It also is meant to be instructional, answering the question, How do I set up an intelligence program in my company? What is the difference between external threats and internal threats? How do strategies to address external and internal threats differ? I list many specific examples relating to programs that I have experienced and utilized to develop a practical intelligence-based plan to implement change for the better; these examples are meant to assist and guide you to establish a similar intelligence program in your company.

Of course you must bear in mind that an intelligence program may vary from company to company, industry to industry; a car manufacturing company will assess and address some significantly different issues compared to an electrical transmission utility company. The car manufacturer's assets are generally confined to buildings, but the electrical utility company may have in excess of 10,000 miles of transmission lines and substations in remote open locations. For example, the car manufacturer may identify through an intelligence-based assessment that expensive computer parts for cars are being stolen by workers. The car manufacturer can address this problem: Employees can be monitored through closed-circuit TV cameras, and strict controls can be placed on the targeted parts to control the problem.

The key is simple in concept: Evaluate your Security Department and see if your people are capable of implementing an intelligence-based security posture. Also, determine if your management is supportive: Are they educated regarding the benefits of properly gathered, analyzed, and implemented intelligence information? After you garner executive

ITEBOOKS.DIRECTORY

management support and hire a skilled security staff, the importance of an enterprise-wide assessment is critical.

Generally the assessment is designed to evaluate what you need to protect in your organization, whether it is vulnerable to attack, risk involved, how the company can be attacked, and the probability of attack. Finally, what are you going to recommend to mitigate and reduce that risk?

The following incidents were researched from open source reporting and demonstrate the value of an intelligence program that proactively gathers data and analyzes and recommends cost-effective measures to reduce risk. No assessment can measure past incidents and factually say that a robust intelligence program would have prevented any of these events. However, because they did occur and if the company had an intelligence program, the question is, Did the program make recommendations to reduce risk that were not implemented? If so, knowing what you know now about the negative consequences of riding out the risk, would you implement the recommended risk reduction measures? Of course, companies would do so; looking back at an incident always leads to 20/20 vision, and the robust intelligence program is intended to provide 20/20 foresight.

TJX, a parent company of discount stores T.J. Maxx and Marshalls, revealed that thieves had stolen information on possibly tens of millions of credit and debit cards. The company first assessed that its systems had been compromised for about 8 months, but it turned out the exposure existed for almost a year. The incident wound up costing TJX millions of dollars. MasterCard uncovered and announced that up to 40 million credit card holders were at risk of having their data stolen because of a virus on the computers of a credit card-processing company, CardSystems Solutions, which had lowered its security standards and improperly stored the card data, unencrypted, to do research on the transactions. Executives admitted the breach was preventable.

The Bank of New York Mellon simply lost a tape. The missing tape contained Social Security numbers and bank account information on 4.5 million customers.

Heartland, a credit card payment processor for hundreds of thousands of companies, revealed that tens of millions of transactions may have been compromised through the utilization of malware that passed the information that allowed thieves to create counterfeit cards with actual user data.

The Department of Veterans Affairs was having trouble with one of the hard drives in a database array. So, naturally, the agency sent the drive

ITEBOOKS.DIRECTORY

out for repair. Unfortunately, it neglected to erase the unencrypted data on the disk. When the contractor was unable to repair the disk, the contractor simply recycled it—again without erasing—leaving the personal information for some 76 million veterans accessible to whomever next got the disk. The Oklahoma Department of Human Services had an instance of an employee leaving a laptop in a car. The laptop had the names, Social Security numbers, and other sensitive information for about a million people. The car was burglarized, and the laptop was taken in the crime, exposing victims to potential identity theft.

The list of major corporations, charities, and government organizations, including the FBI, Central Intelligence Agency (CIA), and White House, that have been the target of computer hackers and internal and external attacks is extensive and getting longer every day. At least the government entities have intelligence programs that are meant to identify, evaluate, and mitigate risk. However, it must be realized that any capable adversary with the intent to attack also is running its own intelligence program. For some of these individuals or organizations that are highly motivated, planning an attack on your organization might be the only thing that they are living for; revenge for a real or perceived slight has been the motivation for many insider threat attacks. The point is: How many attacks would the FBI, CIA, or White House suffer every day without the intelligence programs that they have in place?

Determining that you can live with an acceptable level of risk based on a comprehensive assessment of all threats, vulnerabilities, and risks is a more fact-based decision than closing your eyes and praying that nothing adverse ever happens to your company or organization. In summary: How many times in your life have you or a member of a team you were on said: "If only we had known that yesterday." The advantage of a robust intelligence program is the information you develop through the assessment, evaluation, analysis, and mitigation techniques as part of that program; this information will assist you in strategic and tactical planning. You will have enough information to make a more informed decision and prevent discovering critical facts after the incident. I am a "true believer" and want you to succeed; I am confident that the more people who see the advantages of an intelligence-based security posture in private security, the more we can protect the people and assets entrusted to us in our critical but often-forsaken role as security professionals.

ITEBOOKS.DIRECTORY

ABOUT THE AUTHOR

Tom Trier served 25 years as a special agent of the Federal Bureau of Investigation (FBI), including 13 years in the FBI management program. He attained the rank of assistant special agent in charge in the Intelligence Branch of the FBI Washington Field Office. Mr. Trier's field of expertise was investigating criminal and terrorist enterprises, including extensive service overseas and development of Intelligence programs.

Mr. Trier served 2½ years as the leader of corporate security for a midwestern electrical transmission-only utility company. He was accountable for managing security projects and processes across the company to enhance overall security and reduce corporate security risk. Mr. Trier developed a security intelligence program that defined and analyzed internal, external, and electrical industry threats to the enterprise and formed collaborative working groups to reduce risk through a well-developed security plan.

Mr. Trier provides advisory services through Security Intelligence Consulting LLC.

ITEBOOKS.DIRECTORY

ITEBOOKS.DIRECTORY

Section I

Introduction

ITEBOOKS.DIRECTORY

ITEBOOKS.DIRECTORY

1

Intelligence Descriptions

Depending on your occupation and the mission or objectives you are trying to accomplish, the word *intelligence* has many meanings. A business will utilize intelligence to protect its reputation and develop a strategy to either get on top or stay on top. Military intelligence will gather information to defeat an enemy. In the last few years, cybersecurity across all industries has been applying these techniques to gather information and provide methods to reduce risk through aggressive intelligence programs. The concept of applying intelligence to protect a company's people and assets in a physical security environment is the concept that is discussed in depth throughout this book.

For the military, intelligence concentrates on discovering, evaluating, and exploiting the enemy to defeat them on the battlefield. Knowing where enemy units are, their numbers, and their weapon and communication capabilities is the basic intelligence mission of the military. Of course, for the intelligence capability of modern fighting forces in large countries such as the United States, the military intelligence mission extends to knowing specific enemy units, their morale, and their combat experience, including the outcome of battles they have fought. Who are their commanders? What is their background and combat experience? How well trained are the commanders? How well trained are their troops? The bottom line for military intelligence is how to use information, tactics, and timing to gain the edge on the enemy. The techniques to gather information for analysis range from satellite photographs to the interview or interrogation of captured prisoners.

An excellent example of the utilization of military intelligence in World War II was the American-British operation that put documents outlining

ITEBOOKS.DIRECTORY

the invasion of Europe on the dead body of a British officer and ensuring he was placed where the Germans had a high probability of finding his body. The details on the documents outlined the invasion force landing at Calais and not Normandy, France. Due to this and other items of intelligence, Hitler was convinced the Allies were landing at Calais and did not reinforce the Normandy coast in June 1944, despite Rommel's vehement requests. The Normandy invasion was sketchy enough without the extra Panzer divisions that Hitler denied Rommel; the outcome of the battle may have been disastrous for the Allies had the extra tanks been deployed while the Allies were still trapped on the beaches. The use of military intelligence is geared to an offensive posture: When are we going to attack the enemy, and what is the assurance of victory? The objective is to reduce the risk of defeat through accurate analysis of intelligence.

When gathering data and analyzing for business intelligence, the focus is on evaluating trends in markets, consumer wants, product comparison to the competitor's, company comparisons to industry trends, and whether the company is evolving and staying on the cutting edge. Who is the company competing against, and what are the competition's strengths and weaknesses? How do these compare to our strengths and weaknesses? What are the major competitors doing that is cutting edge, and is this successful for them? Do we do the same thing?

Think of one of the most significant disasters of the twentieth century: A hugely successful soft drink company decides to change the recipe of its basic product and market its new product. It did not work, and the public lost a lot of trust in the company. Even when the company tried to go back to the old product, the damage to the public trust remained. It has taken years for them to recover. It makes you wonder if they had done more testing and a smaller rollout of the new product would they have had enough intelligence to prevent the overall disaster.

The focus of this book is the utilization of intelligence based in private security; what is proposed is the development of an intelligence program that allows a company (Security Department) to gather data, analyze, evaluate, and apply measures to reduce risk based on the factual analysis. For insider threats, if a company is aware of a "problem" employee who has physically threatened other employees, is there a group within the company to evaluate the threat that may be posed by this person? Is this group capable of engaging in a background check of this person to determine if there is a history of violence? Does the person own any guns? Has the person made any statements that may indicate he or she may become an "active shooter?" Are there techniques the company can apply

ITEBOOKS.DIRECTORY

to mitigate this situation, such as suspend the employee until appropriate anger management classes are completed? Are there "trip wires" that can be put in place to monitor this person's computer and physical activity? Or, is the company doing what numerous companies do, subscribing to the thought: "Oh, that is just the way Jim is. He is a crabby person." Too many companies mitigate risk through the statement: "That is not going to happen here; don't worry about it."

Another area of concern in today's world is threats from the outside, external threats. In the example of the soft drink company changing its product, do you not wonder how many death threats were received from the fringe that loved their soft drink as it was and the company changed it without asking them personally: "How about I get my rifle and come down there?" I am sure every company that ever existed has made someone mad, angry enough to make threatening statements. Do I think that every one of these persons is capable of conducting an attack on the threatened company? Of course not, but that does not mean that I would not track every threat and analyze to the best of my ability the capability of the person making the threat. If the person is threatening your company, intent to harm the company is demonstrated. It may just take some time before the person develops the capability to carry out the attack. That is the point: You do not know who is going to attack you if you do not track the threats that come in and continually assess the intent and capability of those who make the threats you are tracking. As intelligence is gathered on these threats, you will be amazed how one small piece of information completes a puzzle that will allow you to act in an informed manner that may prevent a catastrophe.

There is an offensive and defensive nature to all intelligence, whether military, business or physical security, the gathering of data, its analysis and the practical application of conclusions drawn from the analysis is the goal. Developing a robust intelligence program means making informed decisions to act before your adversary.

ITEBOOKS.DIRECTORY

ITEBOOKS.DIRECTORY

2

Intelligence Background

To help explain what an intelligence program is in the context of private security and the value that it brings to private industry, I provide some of my background and experiences. I spent 25 years as a special agent of the Federal Bureau of Investigation (FBI); the dates are important due to the major events that happened during my FBI service from 1986 to 2011. I was sent to the Seattle office after completion of the 17-week FBI New Agents Academy in Quantico, Virginia. I was assigned to the Violent Crimes Squad and worked a variety of violent crimes, bank robberies, extortions, kidnapping cases, bombings, and domestic terrorism investigations. At the time, the small-to-medium offices of the FBI contained only new agents and the most senior of agents who had enough seniority to obtain the "office-of-preference" transfer, which meant they were close to retirement. Agents then were required to retire at age 55; in 1990, they raised the mandatory retirement age to 57.

The core of FBI agents, those with 5 to 20 years service, was in the "top 12" offices; new agents were transferred to these top 12 after around 5 years. In January 1991, I was transferred to the Los Angeles office. Los Angeles was the bank robbery capitol of the United States, experiencing over 2,800 bank robberies a year at the time. I was assigned to work bank robberies in the West Covina Resident Agency (satellite office of Los Angeles), which averaged about 400 bank robberies a year. Drugs such as cocaine and heroin played a major part in the bank robbery problems at the time. Addicts would fuel their habits through a series of bank robberies, sometimes more than 20 committed by one person. We spent our time trying to identify serial bank robbers and charge them with enough robberies to keep them off the streets. We also noticed a large number of

ITEBOOKS.DIRECTORY

African American adolescents were robbing banks in violent and spectacular ways.

Then, we identified a trend: Rolling 60s gang leaders were using bank robberies as initiation tools for young gang member wannabes. They would supply these young men with firearms and tell them to rob the banks and give the money to the gang leaders. The inexperienced robbers would shoot up the banks, strike tellers, and stay in the banks too long. The police would show up; often, the robbers were shot, and sometimes they were killed.

These robbery investigations were some of the earliest experiences I had with the utilization of intelligence paralleling the FBI's traditional investigative techniques. Concentrating investigation and prosecution on the gang leaders behind the robbery initiations contributed to the reduction of bank robberies in Los Angeles in the 1990s. Of course, it was not the only factor: Banks concentrated their assets and bought each other out; they closed many branches, added extra security, and trained their personnel regarding bank robberies, which assisted in the reduction of these events.

In 1994, I was reassigned to investigate Mexican drug trafficking organizations (MDTOs). This was significant as it was the first opportunity I had to formally investigate criminal enterprises. The FBI required a link to an international group to open a drug case; FBI headquarters (FBIHQ) did not want to expend FBI resources on local street dealers. Therefore, you had to develop hard ties to MDTOs such as the Arrellano-Felix Organization or the Joaquin Guzman Organization; this required street agents to coordinate with local law enforcement and develop intelligence regarding the targeted group prior to opening a formal investigation. These investigations also were coordinated with the Drug Enforcement Agency (DEA); as they were the primary agency dealing with narcotics investigations, the FBI did not want to get into a "blue-on-blue" (cop-vs.-cop) situation. The FBI did not want to be buying 25 kilograms of cocaine from the DEA or become involved in an armed confrontation with other cops.

The intelligence gathering of the MDTO investigations was the basis of the intelligence activities that I would utilize in Iraq in 2007 while investigating terrorist cells. For example, the steps in finding out who we were targeting, finding their true backgrounds and defining their capabilities, connections, enemies, family members, weaknesses, and vulnerabilities did not change from enterprise to enterprise. The major difference was the element of intent; in the criminal world, intent was always implied: Because the criminal was breaking the law, intent was easy to prove. It

ITEBOOKS.DIRECTORY

was a little harder to prove in some of the terrorist or private-sector investigations that I conducted, which is discussed further in this book.

By 1997, I began working gang investigations in the Los Angeles area, specifically the Nazi Low Riders (NLR), a white supremacist gang with ties to the Aryan Brotherhood. By now, I had become familiar with the basic principles of the criminal enterprise theory of investigation and readily applied it to this group. At that time, the NLR totaled about 2,500 members in California and Nevada. The first order of business was to form a task force; the Ontario, California, Police Department had five persons working with the DEA as the NLR was manufacturing and distributing crystal methamphetamine in major cities in California to finance their operations in and out of the California Department of Corrections (CDC) facilities. However, the amounts of meth they were dealing were nowhere near the amounts being brought up from Mexico from the MDTOs, so the DEA relinquished the case to the FBI. The CDC had a Special Services Unit (SSU), which assigned a person to the task force, as did the Fontana and Upland Police Departments, along with the Bureau of Alcohol, Tobacco, Firearms, and Explosives, which lent an agent part-time on an as-needed basis. The U.S. Attorney's Office had already assigned an extremely effective assistant U.S. attorney to the case. The FBI gave me two newer agents, and the NLR Task Force was formed with over a dozen law enforcement officers. Its mission was the disruption and dismantlement of the NLR as an effective criminal enterprise.

With the task force officially formed, the next steps were the identification of the leaders of the NLR who were making things happen. As with the MDTOs years earlier, to find out who we were targeting, their true backgrounds, their capabilities, their connections, their enemies, their family members, and their weaknesses and vulnerabilities. I had to demonstrate leadership in this area; the police officers wanted to concentrate all their efforts on making new cases, and I (and the US attorney) wanted also to collect and review historical cases related to the 16 NLR leaders to utilize RICO (Racketeer Influenced and Corrupt Organizations) Act charges in relation to the leadership, so I proposed a compromise. Two days a week, the entire task force would review assigned cases under my supervision, and three days a week, we would pursue new cases the police were investigating regarding NLR members.

The investigation would concentrate on the leaders of the NLR, but the street-level enforcement would continue; we called it "hooking and booking." It was good practice and a specific deterrent; knocking down NLR members' meth houses and putting the members in jail on local or

ITEBOOKS.DIRECTORY

state charges were daily maintenance, but they also supplied us with an extremely valuable and strategic resource: Call them informants, sources, snitches, or whatever, the information gleaned from NLR insiders was invaluable. Knowing what the NLR was doing before the group was doing it was the best example of intelligence gathering, analysis, and application that I had experienced at the time. The intelligence network we built included every law enforcement agency with a footprint in California, a network of over 30 working informants, analysis from the Joint Drug Intelligence Group (JDIG), and an operational arm of 12 officers/agents.

In August 2001, I took a promotion to supervisory special agent (SSA) in the Safe Streets and Gang Unit (SSGU) at FBIHQ. The SSGU was responsible for administrative oversight of all FBI gang investigations across the United States. The SSGU was also responsible for developing and implementing strategy to target the most dangerous and organized gangs with the potential to become a national threat. The intelligence lessons learned in Los Angeles were reinforced while at FBIHQ; reading, evaluating, and analyzing all the gang intelligence that poured into the FBIHQ with the mission to determine the gangs with potential national impact were invaluable to me. They gave me a strategic view and developed my strategic long-term planning skills. Then, the events of September 11, 2001, also happened in the 2-year period I was at FBIHQ, which also had an impact on the FBI missions.

The lessons I learned as an FBI agent in applying criminal intelligence through the criminal enterprise theory of investigation progressed from investigating bank robberies, to drug trafficking organizations and gangs in Los Angeles, and as an SSA in the SSGU at FBIHQ were the basis for the tests that were to come: application of these techniques to terrorist groups in Iraq in 2007. In 2008, I received another promotion and became an intelligence assistant special agent in charge (ASAC) of the Washington Field Office (WFO) in Washington, DC. The time that I spent as the Intelligence ASAC at the WFO truly solidified my skills, and anything that I now do has an intelligence level view applied, and critical thinking through comprehensive analysis is a way of life for me. That is the objective of this book: to show you how I applied these techniques to my civilian jobs and as the security lead at a transmission-only electrical utility company and later as a security coordinator at another major midwestern company.

ITEBOOKS.DIRECTORY

3

Advantages of an Intelligence-Based Program

INTRODUCTION

As stated previously, my personal experience in the intelligence-based posture was obtained from 25 years as a federal law enforcement agent; my expertise was disrupting and dismantling criminal and terrorist enterprises. The importance of identifying, evaluating, and mitigating existing threats and vulnerabilities has risen to the forefront in the analysis of criminal and counterterrorism investigations in the government and public sectors. As I transitioned to a position as the security lead in the electrical utility industry, specifically through employment at a transmission-only company in the Midwest, I realized the intelligence-gathering and analysis techniques applied in criminal enterprise investigations could be applied to private security. The company I worked for had assets consisting of over 10,000 miles of transmission lines, a few hundred electrical substation sites, and about a half dozen offices.

When I started in 2011, I conducted an assessment of the company's physical security program, which was updated on an annual basis. We assessed evolving threat streams and mission priorities. I assessed the capability of personnel to accomplish their missions and together we assessed evolving threat streams. I strove to further develop and document the physical security program, with the task to analyze or advise and recommend physical security measures to company departments and personnel in a collaborative manner. We developed an assessment template (Figure 3.1).

ITEBOOKS.DIRECTORY

Figure 3.1 Assessment cycle.

Some of the initiatives in the company's physical security program under my tenure are discussed next.

SUBSTATION BREAK-INS/COPPER THEFT PROGRAM

The first of the intelligence-based initiatives that we implemented at the company involved substation break-ins and copper theft. Late in 2011, the Security Department conducted an assessment of the company's substation break-ins related to copper theft, utilizing data that included maps and theft information for past years, Security documented and tracked key elements, including but not limited to known copper thieves, nefarious scrap dealers, and law enforcement detectives. Security individuals utilized the gathered intelligence to mitigate or reduce thefts through collaborative programs with law enforcement and other key departments.

INSIDER THREATS

In 2012, Security conducted a collaborative assessment and led the effort that initiated an Insider Threat Working Group, with members in the core group from the following company departments: Physical Security, Information Security, CyberSecurity, Human Resources, and Legal. The team developed a capability matrix of positions in the company and

ITEBOOKS.DIRECTORY

the ability to do harm from that position. We convened the working group on a monthly basis, and when an employee or contractor appeared to develop intent, assessed the situation and developed or implemented controls to monitor the internal threat until the situation stabilized.

EXTERNAL THREATS

In 2012, Security conducted assessments of who would do the company harm; the collaborative effort pulled from available company data and compiled relevant threat information into usable reports or spreadsheets. Security utilized the gathered intelligence to mitigate or reduce threats through collaborative programs with law enforcement and other key departments. Security compiled threat assessments specific to each person deemed to be a threat and communicated these awareness reports throughout the company, including mapping the information to a geographic information system (GIS).

SUBSTATION HARDENING INITIATIVE

In 2013, after the California electrical industry substation shooting, Security worked with asset management and initiated the Physical Security Assessment Working Group (PSAWG). The PSAWG was formed to assess and indicate the cost of all mitigations to physical security vulnerabilities from a coordinated attack of an entire substation, including the substation perimeters, transformers, and the control houses. Based on specific risk assessments, the PSAWG emphasizes utilization of multiple industry best practice mitigation recommendations. Many of these practices include addressing resiliency and a "blended" approach between physical and cybersecurity.

PHYSICAL AND CYBER SECURITY

Also in 2013, Security and Cyber Security coordinated security efforts between company departments dealing in the physical and cyber arenas. The goal was to assess and defend against the cyber-led attack that defeats physical security measures or the physical-led attack designed to gain access to cyber assets. Security and Cyber Security Departments agreed

ITEBOOKS.DIRECTORY

to evaluate developing collaborative assessment tools and in the future developing collaborative incident response plans.

Those five sections were implemented over a three-year period and were the result of several assessments conducted specifically addressing each of the categories. The basic principle for developing an intelligence-based security posture is to develop sufficient situational awareness to determine who is intent on doing your organization harm. Ask yourself these questions: Who is your potential adversary? What is the adversary's capability to cause you harm? Do they have the intent to cause you harm? Where are you vulnerable? How could anyone harm your organization if they wanted to do so? The ancient but applicable axiom, "know your enemy," still applies. Tracking threats and vulnerabilities specific to your organization is the key to minimize risk and damage that may be caused in any attack.

The goal is to develop and maintain a list of subjects or groups capable of an attack and who have the intent to do your organization harm. Armed with this information, if an attack on your organization occurs, quickly turning the list of names of the tracked adversaries over to appropriate law enforcement officials may lead to the rapid arrest of the responsible parties and could be the difference between one or two attacks or a multitude of devastating attacks severely affecting your operations. Examples of types of threats to evaluate for risk reduction include, but are not limited to, insider threats, external threats (specific to your organization), industry threats (specific to your industry), regional threats, national threats, and international threats, described as those by criminal, terrorist, or extremist groups.

Before launching into an intelligence threat assessment, it is imperative to assess the abilities of your security program. Contract guard and alarm-monitoring services do not provide the usual personnel capable of gathering, analyzing, and acting on threat Intelligence. You must determine if the personnel within your security program are capable and willing to initiate and maintain a comprehensive intelligence-based security posture. In our experience, this was a painful and difficult process; personnel not familiar with intelligence-based initiatives were not willing to adapt and were replaced.

ITEBOOKS.DIRECTORY

4

Corporate Security Capabilities Assessment

Throughout this book, "assessments" are discussed; I believe it would be prudent to discuss what I describe as an assessment. We assess everything that we come across in our daily lives. For example, who does not wake up and think about the day to come? For instance: "Today, I have a meeting with human resources to discuss contractor badge clearances. I hope the human resources manager is prepared and stays on topic. Oh, and I have a lunch appointment with Detective Jones to go over the rash of burglaries at our warehouses. I hope that Jimmy, the CCURE technician, took care of obtaining bids on the proposed upgrade to CCURE 2000." Every day, we go over in our minds what we have to do and what we need to accomplish; we are constantly assessing our lives, jobs, and the world around us, mostly unconsciously. We are often distracted by unexpected events and have troubling focusing on long-range goals and improvements.

The assessments discussed throughout this book can range from program assessments, to threat assessments, vulnerability assessments, and risk assessments, but the basic premise is the same: Identify a need or area of opportunity for improvement, define objectives (what you are assessing), develop a methodology, identify assessment team members, make assignments, make a plan, develop a timeline, meet with affected departments, and execute the plan to conduct the assessment. Document everything; the initial assessments of your security and intelligence programs will be the most difficult, but you will find that many of the

ITEBOOKS.DIRECTORY

problems, issues, and opportunities you discover in the initial assessments will be relevant in future assessments. As you are investigating, analyzing, and evaluating any type of criminal activity, you will most likely come across other criminal activity that may not fit into the objectives of your original assessment. This should be documented for pursuit in the future; it will come up again and may also be a valuable piece of a puzzle in future assessments or external/internal threats.

The following is a general methodology template for conducting and planning an assessment of your security program and staff:

- Conduct interviews and collaborative meetings with Corporate Security staff members to determine past practices and engage them in the assessment process.
- Review and evaluate existing documents regarding the past Corporate Security missions. (What did they do in the *past*?)
- Review and evaluate Corporate Security staff job descriptions and comparisons to past Corporate Security missions. (What was the staff told their job was in the past? Present?)
- Review and evaluate current procedures, processes, and guidelines of Corporate Security and ensure they are up to date and compiled in a manner that is user friendly for company personnel. (What are they using now for paperwork?)
- Review and evaluate the financial budget for Corporate Security and compare to ensure the budget is in line with the Corporate Security mission. Ensure programs funded are necessary and not obsolete. (Budget can be the key to improvement.)
- The Corporate Security leader should "shadow" personnel and spend time working directly with all Corporate Security staff members to obtain firsthand knowledge regarding each security personnel's daily duties. (See for yourself and get to know your people.)
- Review and evaluate any compliance tasking assigned to Corporate Security.
- Review, evaluate, and coordinate Corporate Security requirements with the Information Technology Security Department and all other company entities with security cross functionality.
- Conduct interviews and collaborative meetings with other department heads and members of their staff regarding their views and opinions of Corporate Security.

ITEBOOKS.DIRECTORY

Define and review security requirements within the Corporate Security missions and analyze for "mission creep." (Is your Security Department assigned nonformal duties that take away from their primary missions?)

At the end of the assessment, you should have a comprehensive document that delineates an area of concern or opportunity that tells the story of what you were assessing, why you where assessing it, what you found, how you found it (methodology), and how to address it through practical, cost-effective recommendations to management to show improvement, reduce risk, and provide a safe environment for your company. The following is the 2011 Corporate Security Executive Summary prepared for company executives after the initial Corporate Security assessment:

> The following is an Executive Summary of the evaluation and assessment of the missions, capabilities, duties, and responsibilities of the Company Corporate Security Office. This document is intended as a summary of the 2011 Corporate Security assessment, which will be attached to this document for reference.
>
> Analysis has determined the former long-term leadership of the Corporate Security Office, although unintentionally and without malice, lacked several key components to an effective unit; there was a lack of a sense of mission, focus, organization, clear direction, leadership, structure, and discipline. There is an identified lack of a central repository of written standard operating procedures and processes to accomplish the simplest of duties within the department. The Corporate Security Office currently consists of several individuals working in several separate directions but does not constitute a comprehensive team focused on any one mission. Therefore, it is imperative the entire Corporate Security staff concentrate on accomplishing the core missions prior to assuming any other responsibility or duty.
>
> Throughout Corporate Security there exists an immense amount of "tribal knowledge"; the everyday Security Office operations depend on legacy Security staff who know their duties and carry those duties out, but many of these daily duties have not been documented. This has led to confusion from other company departments as some of these processes change depending on who they speak to in Corporate Security. This issue can and will be addressed by the compilation of a Corporate Security Manual of Operations, which will document and organize Corporate Security processes in one Manual of Operations for reference of all personnel, not just Corporate Security.
>
> Through interview and investigation, it has been determined the Corporate Security staff has been self-taught regarding their security

ITEBOOKS.DIRECTORY

duties. The roles of security specialist and security coordinator have delineated job responsibilities as set forth on their job posting from Human Resources; however, interviews with Corporate Security staff indicate most of the staff learned their positions from experience and did not receive any formal training regarding their roles.

Further investigation of the Corporate Security dedicated network t:drive failed to locate any documented formal security training in any areas. Although this does not reflect negatively on the Corporate Security staff, it does indicate there may be a need to evaluate training needs of the Corporate Security Office and provide any formal security training deemed necessary to assist in future operations of Corporate Security.

Analysis did not determine Corporate Security to be completely ineffective or inefficient; there have been significant Corporate Security contributions to the company. For example, Corporate Security has assumed responsibilities in the NERC CIP [North American Electrical Reliability Commission Critical Infrastructure Protection] compliance realm. Corporate Security has had a significant role in the CIP Phase I Substation project and has prepared for CIP Phase II, which will involve enhanced physical security in additional substations. Corporate Security has initiated/participated in several successful asset protection missions regarding substation break-ins, thefts, and protection of construction lay-down yards.

However, analysis has determined implementation of the following steps will improve the overall operations of the Corporate Security Office:

1. Establishment of a team atmosphere in Corporate Security by developing a true sense of mission, focus, organization, structure, and discipline.
2. Corporate Security personnel should be cross-trained in Corporate Security positions to eliminate "irreplaceable experts."
3. Corporate Security will concentrate efforts on the three core missions of physical access control, asset protection, and compliance.
4. Compilation of a Corporate Security Manual of Operations to document in a central repository the standardization of Corporate Security policy, procedures, processes, and guidelines. This will allow existing programs to be evaluated and gaps in the Corporate Security Office to be identified and appropriately addressed.
5. Conduct/document an annual assessment of the Corporate Security missions, capabilities, duties, and responsibilities and evolve as necessary to anticipate and meet future corporate needs in the security arena.

ITEBOOKS.DIRECTORY

6. Evaluation and establishment of a formal training process for existing and future Corporate Security personnel.
7. Define, develop, and meet challenging 2012 goals for the Corporate Security Office.

It is anticipated throughout the coming year as the above listed objectives are accomplished the Corporate Security Office will develop into a more structured, focused, and organized team of professionals with a clearly defined mission. As the team solidifies, the effectiveness of the Corporate Security staff is anticipated to improve, and overall operations are anticipated to reach higher levels.

The development of the plan, methodology, and execution is only the prelude to the hard work that it takes to make improvements and evolve with the ever-changing security environment. Any recommendations that are adopted must be flexible enough and be constantly evaluated to ensure the changes are not obsolete before they can be fully implemented.

This assessment was well received by management, and plans were developed and supported by the company.

As another classic intelligence example from history, after World War I the French built the Maginot Line on their border with Germany to prevent an invasion by German forces. The Maginot Line was an expensive project with concrete bunkers and fixed gun positions; it was impressive but built with the World War I trench warfare thinking. Over the years leading to World War II, the Germans had developed the concept of the *blitzkrieg* or lightning war, which utilized highly mobile mechanized divisions. In 1940, the German mechanized panzer (tank) divisions drove around the Maginot Line, bypassed the bulk of the French Army, and quickly conquered France. Do not build any Maginot Lines into your security or intelligence programs (Figure 4.1).

ITEBOOKS.DIRECTORY

Figure 4.1 The company I worked for had 10,000 miles of transmission lines.

ITEBOOKS.DIRECTORY

Section II

Assessing the Security Program

ITEBOOKS.DIRECTORY

ITEBOOKS.DIRECTORY

5

Evaluate Capabilities

To reiterate, an initial assessment of your security program within your organization, along with personnel and their capabilities, is critical to the effective implementation of your intelligence program. Whether the Security Department is legacy, newly formed, or perhaps nonexistent in your organization, it is imperative that an initial assessment of the Security Department or security program be conducted to determine past practices along with present operations. With the past and present operations clearly documented, future strategic and tactical planning of the security program can be outlined. However, the initial analysis must include an accurate evaluation of personnel and daily operations to determine the capabilities and willingness to adapt to inevitable changes.

Perhaps the Security Department you are inheriting has a highly engaged, motivated, experienced staff with a written set of up-to-date procedures that allows the department to run as efficiently as a Swiss watch. The equipment you have is cutting-edge analytically capable Internet protocol camera systems and every door on your campus has in/out card readers that operate with every swipe of the security-aware and -engaged general population of your enterprise. If this is the case, just skip forward to the intelligence assessment chapters. If you have come into a security program that has poorly trained, self-taught staff with no experience, bad attitudes, and a general population that sees security as a joke, read on.

As I stated previously, when I first arrived at the utility company, one of the first things I did was conduct an initial analysis of my company's security program; I determined the Security Office lacked several key components to an effective unit. There was a lack of a sense of mission, focus, organization, vision, leadership, structure, and discipline. There

ITEBOOKS.DIRECTORY

was no central repository of written security standard operating procedures and security processes to accomplish the simplest of duties within the department. There was an immense amount of "tribal knowledge"; the everyday Security Office operations depended on legacy security staff knowing their duties and accomplishing daily tasks. However, many of these daily duties were not documented. This led to confusion from other company departments as some of these processes changed depending on who they spoke to in security. The Security Office consisted of several individuals working in several separate directions but did not constitute a comprehensive team focused on any mission.

For additional specific background, let me provide some more details specific to the situation I found when I arrived. There were two legacy persons running the security program; one was in charge of "field operations," and the other person did everything else: compliance, physical access, facilities physical security. The former security manager was a hands-off individual who allowed the staff to set their own mission parameters and execute those parameters as they saw fit. There was no sense of set missions, no program management, and no standard operating procedures for daily operations.

The measure that I personally apply to evaluate staff is to judge two aspects, capability and willingness. If a staff member is willing but needs to be trained to develop or hone their capability, they will progress and can be made a valuable member of your team if you take the time to mentor the individual. However, if you have the most capable person unwilling to engage or become part of the team, it is extremely difficult to assimilate this person in your team. Take the time to work with the individual but document his or her actions because if they continue to resist change, they must be replaced.

The legacy staff had dug in their heels and doggedly stuck to their positions and were not willing to adjust. One of the legacy persons was openly hostile; the other had put on an air of cooperation and change but was surreptitiously undermining my every move.

Of course, the legacy personnel saw me as a threat to the status quo. They had never been challenged regarding what they were doing and how they were accomplishing even simple tasks. When one of them was out of the office, the rest of the staff would answer questions with such statements as, "That is Jimmy's job, and he isn't here right now, so call back tomorrow. No, I don't know how to issue a badge, sorry."

The power of the legacy staffer was that only this staffer knew how to do their job; it was not in their best interest to have other people trained

ITEBOOKS.DIRECTORY

in their area of expertise, or they would lose value. Along these lines, processes and procedures were also not written down. If these are written, people can hold you to the standards; if they are not written, you have leeway in the interpretation of duties from situation to situation. If someone challenges, "That isn't what we did last time," it is much easier if things are not written down to say, "Yes it is; that's the way we always did it." Anyone who builds such a power base that sets them up as the only subject matter expert at any company may be perceived as a "gem" because no one really has the expertise to challenge them. They are extremely dangerous as they will do everything they can to derail your plans.

I had to maneuver through setting the standard with overall expectations and used group and individual counseling with each staff member. I initiated monthly staff meetings with set agendas and was candid with the team regarding what was expected; I attempted to engage the staff in the vision of a professional security department. I assigned specific tasks and held people accountable to accomplish those tasks. I measured their engagement and quickly addressed problems when they arose. I assigned one of the legacy staff to compile a security manual of operations that documented and organized security processes in one Manual of Operations for reference use by all company personnel, not just those in Security. I walked the person through the process and attempted to share the vision of a finished product and the benefits of standardized operations.

The following is the speech that I had prepared and presented to the Security staff when I was conducting the initial assessment and had identified but not officially documented the issues. I wanted to set the tone and put people on notice:

Subjects for 11/17/2011 Meeting

Any time a new boss comes into a department, whether it is the military, public, or private sector, it is important the new boss will lay out their vision and set the parameters as to what is expected by their staff. To ensure there are no misunderstandings, I wanted to ensure we all were clear on my positions and communicate the baseline of what I expect from Corporate Security personnel.

1. I am going to provide structure/focus to the department through the evaluation of our core missions, personnel assignments, and job responsibilities. I will be very involved in the day-to-day operations of the Corporate Security Office until I feel comfortable with practices and procedures.

ITEBOOKS.DIRECTORY

2. I would like everyone to utilize the chain of command. I am not saying you do not speak to anyone in the company, but if you are meeting with other managers or executives outside the company, make sure I am aware of the purpose of the meeting and who is in attendance. Do not set up meetings with management without letting me know first; I may have input I would like to discuss prior to setting up meetings.
3. Do not take on any additional projects without discussing them with me prior to committing Security resources. I want to be aware of any new projects we take on and track them.
4. Please make sure you tell me about the content of meetings that you wish me to attend prior to committing to my attendance. Do not schedule meetings for me without asking me first.
5. As time goes by, I will be evaluating each person in the Corporate Security Office, and as we develop a mutual trust, I will determine who earns works without strict supervision and who requires additional coaching.

There was another significant problem the legacy staff had allowed; I call it "mission creep." Basically, if there was something that no one else in the company wanted to do (i.e., background checks on contractors), it was given to Security. As things evolved, it eventually was believed that Security was responsible for every aspect of contractors, including training, background checks, clearance levels, even contracts. Because of this mission creep, there was also a bifurcated training process at the company; Human Resources assigned employee training, and Security rolled out training for "nonemployees." The company allowed two totally different methods of training, including tracking; it was confusing and problematic. The company background checks included a component that was federally regulated under the North American Electrical Reliability Commission (NERC) Critical Infrastructure Protection (CIP) statutes and required training annually and background checks every seven years. Noncompliance resulted in fines and other penalties. The two-tier system was compounding an already-difficult compliance issue (Figure 5.1).

Eventually, several of the legacy security personnel left the department, and personnel with better understanding of basic security operations were hired. Having the right people in the right positions with the right attitude is a winning formula.

The following is the documentation of the initial plan for our assessment:

ITEBOOKS.DIRECTORY

Figure 5.1 Who is protecting the grid?

Corporate Security Assessment

The following is an outline for an evaluation and 90-day assessment to detail in a living document the mission, capabilities, duties, and responsibilities of the Corporate Security Office. Upon completion of this assessment, a comprehensive, clearly defined security summary will be completed; this document will include the Corporate Security mission statement, personnel duties/responsibilities, and financial status. A section of this report will define short- and long-term goals and objectives for the Corporate Security Office. This report will be updated annually or as needed. The following bullet points will be covered in this document:

Define Corporate Security missions:

1. Asset protection
2. Access control
3. Incident management and response (procedures)
4. Intellectual property and sensitive information protection (procedures)
5. Compliance (Critical Infrastructure Protection, CIP) (other)
6. Coordination with all other departments

To clearly define the mission, the following steps (and others to be determined) must be taken:

ITEBOOKS.DIRECTORY

Obtain existing documents regarding the corporate security mission.
Obtain Corporate Security job descriptions and compare to Corporate Security missions; adjust accordingly.
Analyze the financial budget for Corporate Security and ensure the budget is in line with the Corporate Security mission. Ensure programs funded are necessary and not obsolete.
Analyze current processes and procedures for Corporate Security and ensure they are up to date and compiled in a manner that is user friendly for personnel.
Analyze Corporate Security task spreadsheet and compare to updated mission statement to ensure all tasks addressed are documented in the mission statement and job responsibilities.
Pull the CIP requirements and review; keep the CIP requirements updated and easily accessible to all employees.
Coordinate CIP with the Information Technology Security Department and all other entities with CIP responsibilities.
Define other compliance requirements within the Corporate Security mission.
Analyze and review Corporate Security policies and procedures for other bulk electric system companies for best practices to adopt at our company.

With the plan documented, I adopted methodology on how to execute the assessment, which was as follows:

Analysis Methodology

The methodology used to conduct this assessment included the review and analysis of the following:

1. Reviewed and evaluated existing documents regarding the past Corporate Security mission.
2. Reviewed and evaluated Corporate Security staff job descriptions and comparisons to past Corporate Security missions.
3. Corporate Security team leader "shadowed" personnel, meaning spent time working directly with all Corporate Security staff members to obtain firsthand knowledge regarding each Security personnel's daily duties.
4. Reviewed and evaluated the financial budget for Corporate Security and performed a comparison to ensure the budget is in line with the Corporate Security mission. Ensured programs funded are necessary and not obsolete.
5. Reviewed and evaluated current procedures, processes, and guidelines of Corporate Security and ensured they are up to

ITEBOOKS.DIRECTORY

date and compiled in a manner that is user friendly for company personnel.
6. Reviewed and evaluated the Corporate Security task spreadsheet and compared to the updated mission statement to ensure all tasks addressed are documented in the mission statement and job responsibilities.
7. Reviewed and evaluated the NERC CIP requirements to ensure compliance with CIP requirements as they pertain to Corporate Security. It was critical to keep the CIP requirements updated and easily accessible to all Corporate Security employees.
8. Reviewed, evaluated, and coordinated NERC CIP Corporate Security requirements with the Information Technology Security Department and all other company entities with CIP responsibilities.
9. Defined and reviewed other compliance requirements within the Corporate Security mission and analyzed for "mission creep."
10. Identified, analyzed, and reviewed Corporate Security policies and procedures for other electric utility companies for best practices to adopt at the company.
11. Conducted interviews and collaborative meetings with Corporate Security staff members to determine past practices and engage them in the assessment process.
12. Conducted interviews and collaborative meetings with other department heads and members of their staff regarding their views and opinions of Corporate Security.

As a simple but effective guideline for the initial Security Department assessment, ask and answer these questions: What is the structure of the Security Department/program in your organization? Who do you have working for you? What are they doing? What should they be doing? Is there a team or are there several individuals doing their own thing? What does the company expect from Security? What are our core security missions? Evaluate each team member and their position by the simple mantra: Are they willing? Are they capable? Document everything and develop a strategy and vision. Engage your staff or, if they are unwilling, move them out and handpick an engaged, willing, loyal, capable staff and continue to mentor and train them.

ITEBOOKS.DIRECTORY

ITEBOOKS.DIRECTORY

6

Recommend Security Standards

The results of the initial assessment were documented in two ways: a lengthy detailed document and an executive summary. The executive summary was from the initial assessment completed at the end of 2011; it was intended that an assessment would be conducted annually after the initial one to allow the security and later intelligence program to grow and evolve. The growth and evolution were captured in each of the following assessments in 2012 and 2013. A PowerPoint presentation was made to company executives regarding the results of the initial assessment. These individuals were engaged and supportive of the changes that had to be made. Of course, by the time we had the initial assessment completed, we had already been working on some of the solutions. The following discussion presents some of the specific things that we had accomplished.

After the security program assessment, we implemented the following measures to address the opportunities that we identified:

1. We provided leadership and ensured the establishment of a team atmosphere in Security by developing a true sense of mission, focus, organization, structure, and discipline.
2. Security concentrated efforts on the three core missions of physical access control, asset protection, and compliance.
3. Security personnel were cross-trained in Security positions to eliminate "irreplaceable experts."
4. A Security Manual of Operations was compiled to document, in a central repository, the standardization of security policy, procedures, processes, and guidelines.

ITEBOOKS.DIRECTORY

5. This allowed existing programs to be evaluated and gaps in the security program to be identified and appropriately addressed.
6. We conducted and documented annual assessments of the Security missions, capabilities, duties, and responsibilities to evolve as necessary to anticipate and meet future company needs in the security arena.
7. We evaluated and established a formal training process for existing and future Security personnel.

If you determine the staff to be capable and willing, the next step is to engage them in developing missions/objectives. The basic security missions of your company must be evaluated, assessed, and addressed. As part of the development of specific missions, ensure you engage your management for direction; this will involve them in the process and provide them education as you move the security program forward. It is imperative the entire Security staff concentrate on identifying and accomplishing the core security missions. Assess what the company does and how Security would be best positioned to protect the company's most critical assets. Seek other companies in the same industry and engage them to determine what they are doing regarding security missions. Once you have general ideas on the security missions right for your company, develop a plan to engage your employees and make them part of the mission definition process. It will be easier on everyone if the team comes to a consensus and assists in the process.

This will be specific to your company; there are some specific missions that most security programs address, such as physical access control, which involves tracking badges and granting physical access based on a properly documented and executed access request process. Ensure the owners of the business units approve of the access to their assets, not your Security Department. For example, if the Information Technology (IT) Department has a server room, the department should use the access request process to approve or deny access to the server rooms.

Through monthly Corporate Security staff meetings, I collaborated with the security staff and company management to define the three primary missions: asset protection, Critical Infrastructure Protection (CIP) compliance, and physical access control. Once you set missions, ensure you engage security team members to define how to accomplish the missions they are assigned, their duties and responsibilities, and a method to check on them as they move through the process to ensure they are on track and enhancing their program.

ITEBOOKS.DIRECTORY

Document mission statements and assign a leader to "own" each of the security missions. As stated previously, ensure leaders not only are capable and willing to accomplish the missions assigned to them but also are so engaged in their assignments that they continue with passion and zeal to evolve the missions with changing threat streams in the future. We assigned a security specialist to each of the primary missions; there was an asset protection security specialist, CIP compliance security specialist, and physical access control security specialist, each responsible for all aspects of their primary mission.

The missions were documented as follows:

Physical Access Control: Our company has five business offices; some of the offices have physical security perimeters (PSPs) that are protected with cameras, alarms, and badge card readers. Our company also has substations, including substations with PSPs. A total of 250 alarmed doors exist throughout our company; these are maintained through Corporate Security. Corporate Security is responsible for monitoring and controlling varying levels of physical access to company facilities and assets.

Asset Protection: Our Company also has 10,000 miles of transmission lines throughout three states: Wisconsin, Illinois, and Michigan. Corporate Security is responsible for the detection and prevention of risks, including thefts from company assets across the corporate footprint.

Compliance: Corporate Security has roles in North American Electric Reliability Corporation (NERC) CIP compliance, specifically CIP-004 and CIP-006. Corporate Security is responsible for CIP-004, which outlines compliance to standards dealing with the R1 Security Awareness Program; R2 Security Awareness training, conducted quarterly; R3 Personnel Risk Assessments (background checks); and R4 Physical Access/Revocation procedures. Corporate Security is responsible for CIP-006, which outlines compliance in standards dealing with R1, the Physical Security Plan; R2, Protection of Physical Access Control Systems; R3, Protection of Electronic Access Control Systems; R4, Physical Access Controls; R5, Monitoring Physical Access; R6, Logging Physical Access; R7, Access Log Retention; and R8, Maintenance and Testing. Corporate Security also has compliance and audit responsibilities in other areas of CIP and areas outside CIP compliance.

ITEBOOKS.DIRECTORY

Along with defining the missions, I set goals for myself and for the security team through my tenure that were mission specific. These goals were intended to not only advance the missions but also engage willing team members in the vision that I was bringing to the department. The goals were also collaborative and meant to engage other departments with Corporate Security in like missions; this assisted in developing relationships throughout the company. The first sets of goals from 2012 were as follows:

Corporate Security Team Leader 2012 Goals

I will organize Corporate Security operations by supervising the creation of a Manual of Operations for Corporate Security to serve as a central repository for appropriate documents, such as Corporate Security processes, policies, procedures, and guidelines regarding the core security missions, physical access control, asset protection, and compliance. This advances the Corporate Security function by centralizing documents that are Corporate Security standard operating procedures into one location, allowing Corporate Security personnel to organize, analyze, and evaluate existing documents for gaps and author the appropriate documents to address issues that have previously been unnoticed. It is anticipated the initial gap analysis will be completed in the first quarter of 2012. Progress will be measured by the number of gaps identified through the compilation and evaluation of the central repository. The goal will be evaluated by the number of documents written to address the identified gaps. All Corporate Security personnel will have a portion of this team goal assigned to them. Collaboration on this goal includes participants from the entire Corporate Security staff, Facilities, and Information Technology Departments.

I will enhance the Corporate Security copper theft/break-in program through the supervision of Corporate Security personnel, who will conduct scientific analysis of the facts of the thefts gathered through copper theft/break-in investigations, along with the use of geographic information system (GIS) mapping, to develop patterns of criminal activity. This will improve department efficiency and allow Corporate Security to strategically plan proactive measures to combat future copper thefts/break-ins. This advances the organization by adding strategic planning to the deployment of Corporate Security's limited resources. It is anticipated monthly meetings will begin in the first quarter of 2012 and continue throughout 2012. Success will be measured in two categories: by the number of strategic measures developed and by the number of strategic measures implemented by the end of 2012. Included in collaboration on this goal are select participants from the Corporate Security

ITEBOOKS.DIRECTORY

staff, other Wisconsin Utility Company security personnel, and members of law enforcement.

I will improve efficiency by supervising the development of Corporate Security business processes that are defined and repeatable regarding the installation of physical security measures in the substations identified for enhanced security in the Phase II project. This includes authoring guidelines and checklists for risk assessments for the identified substations. This goal includes the writing of standards and templates to meet CIP compliance guidelines. This advances the company goal to ensure CIP compliance regarding these substations and the utilization of Corporate Security documents developed through these business processes. This will be measured by the successful implementation of the newly developed Corporate Security business processes in the risk assessment and execution stages of the Phase II project. The goal will be evaluated by the successful completion of risk assessments on all Phase II substations by the end of 2012. Collaboration on this goal includes participants from the entire Corporate Security staff and departments participating in the Phase II project.

I will enhance the CIP compliance program to reflect the company's strict attitude of compliance. There are CIP responsibilities that have been handled by Corporate Security and with the establishment of the company's CIP Program Office; I will supervise Corporate Security personnel to conduct a complete and comprehensive evaluation/analysis of all CIP programs throughout Corporate Security to determine which CIP programs would be eligible for transfer to the CIP Program Office. The evaluation/analysis will be coordinated with the CIP Program Office to ensure accuracy and a smooth transition. The evaluation/analysis will be completed by the third quarter of 2012. Success will be measured by the completion of the project by Corporate Security personnel and the ability to hand off appropriately identified CIP programs by the end of 2012.

Summarize and document your findings for future reference and to brief executives. Looking back, it seems so simple to me, but I do recall it was a difficult and trying time. The stress of dealing with the personnel issues compounded by the confusion of what was expected from the Security Department by the company was extreme.

It is critical to educate and elicit the engagement of your organization's management regarding the value of your security department and the establishment of an intelligence program. If management does not support such a program, find out in the initial planning stages, prior to devoting resources to a program unwanted by your organization.

ITEBOOKS.DIRECTORY

Once each of the missions is defined, it is imperative you standardize operations and practices and document how each of the missions is accomplished. With each mission writing its own standard operating procedures, it is highly recommended these documents be utilized to create a manual of security operations. This document will allow you to evolve your security team to a truly cross-functional team. If your standard security missions are, for example, asset protection, compliance, and physical access control, the Manual of Operations would contain three sections, each concentrating on the primary missions. All procedures, processes, and guidelines are classified into each of the primary missions. A comprehensive Manual of Security Operations will allow the asset protection specialist to cover for the physical access control specialist (e.g., for issuing a badge). The asset protection specialist should have the Manual of Security Operations for reference, and a step-by-step procedure would be available for the task of issuing a badge instead of telling the person requesting the badge to wait until the physical access control specialist returns.

In the evaluation and analysis of the documents that will comprise your Manual of Operations, pay close attention to the processes and standards that you have in place for granting and tracking access. At both corporate entities where I have been employed since leaving the Federal Bureau of Investigation (FBI), the security component had manual, cumbersome, and archaic methods for granting access and no electronic means of tracking except for scanning the forms to PDF form in a folder. This is an area that needs to be addressed; the granting of physical access should be automated to an electronic format such as SharePoint or Service Desk. These applications have the capability to develop work flows, drop-down menus to specific access levels, and e-mail notifications to approving business managers, who own the space, and to customers who ask for access along with the Corporate Security for access fulfillment before a badge is issued. The assurance that the business owner approves the access prior to you issuing a badge and the fact the requests can be tracked and exported to an Excel spreadsheet greatly assist any compliance requirements. In fact, the advantage of electronic automation of the access approval process crosses all three of the major security missions. Knowing who has restricted, controlled, monitored physical access to your critical access assists the asset protection specialists in any investigation to discover or eliminate any insider threat. Obviously, the physical access control specialist would benefit from an organized electronic access automated process; as stated previously, the compliance specialist

ITEBOOKS.DIRECTORY

will have data available for tracking and audit purposes at the push of a button. Any evolutions to your access levels or standard operating procedures are much easier to revise in an electronic format.

Finally, the Corporate Security leader will have a method to compile the statistics that are valuable to the department and difficult to track manually. The value of hard facts through statistics is difficult to refute when competing for funding against other support groups within your enterprise. Many of the common questions that can be easily answered from electronic tracking of the access statistics are the following: How many access requests do we receive in a year? How many are processed? How many access level changes are there in a year? How many requests are denied? Why? Are there patterns to analyze? How many people currently have access to our most critical assets? How often do we audit these critical access levels? Quarterly?

Any intelligence program that is developed must have an "action arm" that applies the gathered intelligence to a specific mission. Also, a security staff familiar with systems capable of electronic access will be easier to train and adapt to intelligence-based programs and will in fact pursue electronic tracking of intelligence information within their own submissions if they are comfortable with these and similar systems. For example, if you develop intelligence that a certain crime group is targeting your organization by stealing widgets from your warehouses on the third Sunday of the month, having a predetermined plan that enables an asset protection specialist with developed law enforcement liaison contacts to act with the police on that information as part of their job is as critical as the ability to develop the intelligence in the first place. There is the ability to track that information electronically and report to the police in a professional and timely manner.

Also, be aware as you continue to evolve and move toward developing an intelligence-based security posture, you have to constantly evaluate and maintain the core missions of your Corporate Security department. If you denigrate the asset protection mission by moving resources to the intelligence mission without backfill of that position or a realistic review of the asset protection specialist's workload, you may be setting yourself up for some frustrating times. Careful assessment of resources in the establishment of the primary security missions, engagement of your security staff, and engagement of your company management executives are all factors that will affect implementation of defined security missions and new intelligence-based programs.

ITEBOOKS.DIRECTORY

ITEBOOKS.DIRECTORY

Section III

Building Consensus

ITEBOOKS.DIRECTORY

ITEBOOKS.DIRECTORY

7

Initiate Collaboration of Cyber Security and Others

Today, many organizations have separate Cyber and Physical Security Departments, each assessing and addressing their own venues; often, discussions between the two departments are limited. While at the utility company, I had extensive conversations and meetings with the Information Services Security manager; we concluded that the idea of tracking and analyzing external and internal threats across the cyber and physical realms had great merit. Our discussions made us realize that, in these times, most threats involve a cyber and physical capability to carry out an attack.

For example, if an entity develops an ecoterrorist adversary such as the Animal Liberation Front (ALF) or the Earth Liberation Front (ELF), the threat crosses the cyber and physical realms. The ecoterrorist extremists have access to a national network of individuals with similar political ideologies, and they are extremely well financed; some of these groups have committed acts of violence, including arson, fire bombings, vandalism, intimidation, assaults, and stalking. Other members are computer experts and have carried out cyber-based attacks on their adversaries.

We authored the following outline to educate and engage company management:

ITEBOOKS.DIRECTORY

Physical and Cybersecurity

1. Coordinated attack (physical and cyber). Assess and defend against the cyber-led attack that defeats physical security measures or the physical-led attack designed to gain access to cyber assets.
2. Develop collaborative assessment tools. Develop collaborative incident response plans, including, but not limited to, the following threats:
   a. Insider threats: disgruntled employee/contractor
   b. External threat: terrorist, disgruntled landowner, or electrical industry hater
   c. State-sponsored attacks
3. Evaluate the value or necessity of reporting to one centralized chain of command.

We did develop and initiate a collaborative insider threat group, which I describe in depth in further chapters. Unfortunately, due to circumstances out of our control, we did not have the time to expand the external threats program to include a complete analysis of all the external threats we had identified on the physical security side for any cyber attack capability. We did share information with company cyber personnel but did not conduct a joint assessment of any threats they had identified for any physical attack capabilities.

It is anticipated that the future of security will depend on Physical Security and Cyber Security coordinating security in the physical and cyber arenas as a joint effort. The goal will be to assess and defend against the cyber-led attack that defeats physical security measures or the physical-led attack designed to gain access to cyber assets.

Because the majority of physical access control (PAC) systems utilized to monitor physical access are computer based, it is only logical for criminals or adversaries to develop plans that utilize cyber-based attacks to defeat the PAC systems and gain physical access to a targeted organization. Assessments conducted would not be complete without evaluating these attack vectors. Physical Security and Cyber Security should develop collaborative assessment tools; in the future, this effort must include developing cross-functional incident response plans. These plans must include a communications plan that notifies "on call" Physical and Cyber Security personnel of incidents in either venue for complete analysis, evaluation, and mitigation. A joint incident response team with members of Physical and Cyber Security Departments is also highly recommended.

ITEBOOKS.DIRECTORY

Also, as the lead security professional at your company, every day that you come to work, you interact with myriad other departments: Facilities, Safety, Human Resources, Legal, Manufacturing, Office Services, Information Technology, Cyber Security, and the list goes on, depending on your company's structure. No program can stand on one leg. Contact Legal, Human Resources, Business Intelligence, Cyber Security, Information Assurance, Risk Management, Facilities, and Operations. There may be others in your footprint; make it part of your assessment to determine those you interact with.

Security is as integral a program as safety; however, it is not as recognized because real security issues that affect company production rarely occur, whereas the line shuts down if there is a safety incident. The reason I mention this is to ensure you understand the importance of educating your organization regarding the relevance of security.

One effective way to engage the department heads of crucial departments (e.g., Legal, Human Resources, Safety, Information Technology, and Facilities) is to invite them to participate in appropriate assessments. Do not invite them to every meeting regarding the assessment; they are busy also, and if you expend capital by inviting them to every meeting, they will believe you are wasting their time. However, prepare an initial meeting with the objectives of the assessment and allow them to discuss their views, problems, issues, and opportunities with security in an open forum. Document these problems and work on correcting them even if they are outside the scope of your assessment objectives. Once improvements are in place, reengage the departments and follow up with them to explain what you have or your department has done to address their concerns and thank them for their assistance.

As you continue to bolster your security program, ensure you also research insider threats and any actions taken by your company in this area. Many companies consider insider threats a human resources issue and limit the involvement to Legal and Human Resources in the event of an employee with significant life changes that are having a negative impact on their work performance. These departments will develop programs to stabilize or terminate the employee, but they rarely look at the risk the employee may pose in their agitated state; even if these departments become aware of threats the employee may make to harm assets, including people, they are usually not proactive in their approach.

They generally view the situation from their legal or human resources point of view, as well as they should; as the security leader, you should

ITEBOOKS.DIRECTORY

engage them and develop an understanding for their point of view. As you prepare to develop the insider threat program, engage the other departments (e.g., Facilities, Safety, Human Resources, Legal, Manufacturing, Office Services, Information Technology, Cyber Security) in exploratory conversations regarding the insider and external threats and vulnerability assessments.

ITEBOOKS.DIRECTORY

8

Liaise with Industry Partners and Law Enforcement

Working with industry partners and with law enforcement has equal value but different payoffs, and each should not be neglected for the other. In other words, parallel tracks to establish and maintain liaison contacts with your industry partners and law enforcement should begin as soon as possible. The engagement with the law enforcement partners was easier for me with my prior law enforcement background compared to engaging with the other electrical industry security departments. Because I was not a legacy electrical utility security person, I was an outsider to them, and relationships were difficult for me. However, dealing with the police and other law enforcement personnel, such as dispatchers and analysts, came easily to me.

I did not give up on the industry partners; there was a tradition of meeting twice a year to discuss common problems. I attended each meeting and hosted one at our company headquarters site. We had a unique situation with the transmission-only utility company as the other power companies that generated the power utilized us to transmit the power; they were our customers and our owners. It was a subservient relationship; any disagreement with any of the other companies on our part was quickly resolved their way. It was challenging; however, do not misunderstand. Their security personnel were decent people; they just did not have any semblance of an intelligence program or strategic approach to security.

Because we first concentrated efforts on the substation break-ins, transmission line shootings, vandalism, and other criminal activity that

ITEBOOKS.DIRECTORY

required close working relationships with law enforcement, it was clear to me how to engage the law enforcement officials; I knew how they thought and what was important to them.

For instance, regarding the substation break-ins, I asked the legacy asset protection security specialist how they engaged law enforcement in any substation break-in incidents. I was told they would ask the responding officer or deputy, "What are you going to do about this break-in?" The philosophy was to make the responding officer responsible for ownership of the break-in, a clear misunderstanding of how law enforcement works. The response to the break-in may be only one of several responses to incidents the officer went to that day; unless the incidents were related or a blatant clue was found on the scene, the responding officer wrote a report with facts they obtain and submitted the report to detectives. Because many of our break-ins were found in monthly maintenance checks, the break-in could be up to 30 days old. The detectives usually have an extensive case load; the report of the break-in would go to them for analysis and investigation. Unless there was a definite pattern developing of similar substation break-ins in the area, the file sat in a pile until a criminal pattern developed, someone was caught and confessed to the break-ins, or the case was closed after a number of years according to department policy.

We developed an intelligence-based database of known offenders who had been involved in copper theft previously; we started with 20 names, and over a period of two and one-half years, expanded the list to approximately 400 names of known offenders.

As discussed in the next chapter, we initiated and maintained three databases: the detectives/investigators of law enforcement agencies working copper thefts, a database of known offenders, and a list of metal scrap yards that were allegedly nefarious. We would monitor substation break-ins; as substation break-ins occurred, we would look at the area, determine vulnerable substations that were in the area that might be targeted next, and deploy additional cameras and detection devices to those deemed most vulnerable (Figure 8.1). Also, we would look at the detective spreadsheet and determine which detectives in the area would investigate the crimes. We then examined our known offender and scrap yard spreadsheets for the area and met with the detectives, sharing the information on the past criminal activity, specifically names and all the background we were tracking. I had the team author an "action plan" to address copper theft/substation break-ins. The following is the example of the action plan:

ITEBOOKS.DIRECTORY

Figure 8.1 Perimeter fence hole cut by the copper thief.

2012 Copper Theft/Break-In Action Plan

Situation: A recent assessment by Corporate Security has identified a need for a copper theft/break-in analysis and mitigation plan defining Corporate Security strategies and actions.

Mission: In a collaborative effort, the Corporate Security team will create a repository of strategic measures to be considered, prioritized, and implemented in an effort to reduce copper theft and break-ins, therefore enhancing the company's asset protection plan. This advances the organization by applying strategic planning to the deployment of Corporate Security's limited resources.

Execution: Under the supervision of the Corporate Security team leader and in collaboration with Corporate Security staff members, the project lead security specialist will lead the mission to gather intelligence, analyze data regarding copper thefts and break-ins, discuss strategic measures, and prioritize those measures to implement an action plan to serve as a road map of direction toward the reduction of incidents. The team leader, the lead security specialist, and others from Corporate Security or other invited departments have initiated monthly meetings and have begun to assess and brainstorm potential solutions for implementation.

It is anticipated monthly meetings will begin in the first quarter of 2012 and continue throughout the remainder of 2012. These monthly meetings will be the setting for a partnership of Corporate Security and other resources where collection of data or statistics will be continually updated, analyzed, and prioritized. The initial analysis will include the identification of company field assets and mapping incident locations from 2010 and 2011. Going forward, information that will be collected and

ITEBOOKS.DIRECTORY

plotted will be (1) incident coordinates [longitude/latitude]; (2) salvage yard locations, and (3) Phase II substations with enhanced security sites. Throughout this project, other categories may be identified and added to the plotting and analysis. Further examination will be conducted, concentrating on identification of any patterns of criminal activity. This will improve department efficiency and allow Corporate Security to strategically plan proactive measures to combat future copper thefts/breakins. The initial analysis is anticipated to be accomplished by the end of the first quarter 2012, with preliminary steps of action(s) identified and implemented.

This process will continue throughout 2012. Each month, the project lead security specialist will summarize and forward to the team leader the incidents that have happened, what has been discussed and prioritized at the monthly meetings, and the implementations acted on. Progress and success will be measured in two categories: (1) by the number of strategic measures developed and (2) by the number of strategic measures implemented by the end of 2012.

It is expected the entire staff of Corporate Security will be involved to varying degrees in this process. As gaps are identified, the team leader and the project lead security specialist will evaluate the measures identified and prioritized associated with combating incidents and frequency. Assignments will be made based on expertise and departmental needs. Coordination of assignments to other departments will also be recorded and tracked. This tracking will be maintained by the project lead security specialist. The following Corporate Security personnel will be assigned responsibilities and tasks throughout 2012:

1. Team leader
2. Asset protection security specialist—project lead
3. Compliance security specialist
4. Physical access control security specialist
5. Security technical specialist
6. Security coordinator

Command and Control: The Corporate Security team leader and project lead security specialist will meet weekly and additional security staff invited as deemed necessary. At each 2012 monthly meeting, team members will discuss incidents, status, investigations, trends and patterns, strategic options, and assignments and track progress on assigned tasks. In addition, any communications made or joint efforts with other departments, utility company security personnel, and/or members of law enforcement will be discussed and shared. Team leader

ITEBOOKS.DIRECTORY

will periodically report progress to executive management through the proper chain of command.

Administrative: The team leader will assume overall responsibility for this project. Project lead will conduct the day-to-day operations regarding this project and will make assignments to other Corporate Security staff members in conjunction with team leader. Efforts will include collaboration with Geographic Information System, Maintenance, Engineering, along with Wisconsin utility company security personnel and/or members of law enforcement. Progress will be tracked and measured by the number of strategic measures developed and by the number of strategic measures implemented on a monthly basis.

We executed on this action plan and were successful in building significant law enforcement relationships that had a major impact on the copper theft problems we had and reduced the number of substation break-ins from almost 30 in 2011 to less than a handful in 2013. The processes we put in place were repeatable, and we followed the standard, once it was set, to build and maintain law enforcement relationships. Developing and maintaining contacts in the same industry are valuable for you and your staff to ensure collaborative efforts and industry trends. Knowing what other people are doing is a great selling point to your management. However, be cautious as sometimes just because everyone else is doing something does not make it right; many times, the industry is resistant to change, and tracking threats has not been normal business practice. Ensure you communicate with your peers and develop an understanding of their vision for the industry and adjust accordingly.

ITEBOOKS.DIRECTORY

ITEBOOKS.DIRECTORY

9

Show Success

Once you establish a security program, have staff comfortable with their daily duties, and decide it is time to begin the intelligence threat assessment, appoint an individual to take the lead on each component of the intelligence program effort. When I started at the utility company in 2011, one of the biggest problems the company was experiencing was substation break-ins, most of them involving copper theft.

As stated previously, when I asked the security personnel for their incident reports, they told me they did not have any. When I asked for the police reports, they told me "the police reports were too hard to get." I had a person obtain the police reports; 76 reports were obtained for a 5-year period. Once the reports were analyzed, we found the police had identified several suspects of which we were not aware or persons of interest or individuals charged in other crimes, so our company was not notified through the judicial process. However, these were copper thieves that had been breaking into our substations. Based on my law enforcement experience, I believed they would be back because many were charged with misdemeanors and not in custody.

We continued our assessment of the substation break-in/copper theft problem and initiated the following measures:

- Security began meeting the first Friday of each month to analyze incidents from the prior month and develop measures to address any of these issues. These meetings included personnel from Asset Management and other company personnel as deemed appropriate.
- Security obtained and maintained strategic mapping of company theft/break-in incidents.

ITEBOOKS.DIRECTORY

Security developed and documented a standardized incident report form with clear processes; this assisted in tracking and reporting details of incidents.

Security identified, developed, and maintained an incident report database that was easily accessible and provided the ability to analyze data and produce usable reports to identify criminal patterns and activity with the intent of loss prevention.

When definite ongoing patterns of criminal activity were identified, Security utilized strategic mapping to assess the area of criminal activity. Based on the analysis of vulnerable substations in the area, Security strategically deployed their limited video resources in areas of criminal activity to deter the subjects from thefts/substation break-ins. The video systems have been randomly rotated within the area of criminal activity to create the appearances that more units have been deployed than actually are in the field.

Security developed a monthly report to inform managers of theft/break-in incidents. Recipients included company executives, construction, safety, security, and asset management personnel.

Security initiated and maintained three separate spreadsheets for tracking: a list of known copper theft subjects and suspects; a list of scrap dealers, with a tiered system to track the most nefarious; and a list of law enforcement officials investigating copper thefts. This intelligence was shared with other utilities and law enforcement. Law enforcement arrested subjects based on the intelligence we provided them (Figure 9.1).

Figure 9.1 Evidence of copper theft after execution of a search warrant.

ITEBOOKS.DIRECTORY

Security collaborated with Asset Management, and this department coordinated with company finance personnel and developed a cost code for copper theft/break-in repairs to accurately track monetary loss.

Security collaborated with Asset Management and updated the substation inspectors' checklist to include a brief updated security section with their monthly rounds.

Security identified company substations that required fixed video systems or heightened security measures due to the history of past break-ins.

Security authored a security assessment checklist as a guide for Security personnel evaluating construction lay-down yards.

Security collaborated with Construction to formulate a checklist for their use in good security practice in construction lay-down yards.

Security developed and maintained a spreadsheet of all company assets and the level of physical security at each of the offices, substations, or any other company measurable physical asset.

Security evaluated and tested new detection and other cutting-edge technology for value and deployment in the substation break-in initiative. Security added high-definition cameras and infrared beam detection devices to deployable security packages.

The following is an example of a process I developed to track incidents and ensure the staff knew expectations relating to break-in incidents:

Incident Response Processes

The following is a process for the acquisition and documentation of information regarding incidents that fall under the responsibilities of the Corporate Security Office:

1. Receive notification of an incident by any means of communication.
2. Obtain the Incident Response form and start the documentation.
3. The form is self-explanatory; fill out fields on the first page (see the Incident Report form).
4. Upon completion of the Incident Response form, request the caller notify local law enforcement by dialing 911 to report the theft and initiate a police report (if deemed necessary, i.e., criminal activity).

ITEBOOKS.DIRECTORY

5. Follow up with the initial caller to obtain the police report number and police officer's name and agency and complete the Incident Response form.
6. Notify all Corporate Security staff of the incident and send a copy of the incident response form to the Corporate Security team leader for assignment to an investigator.

Upon receipt of the Corporate Security Incident Response form, the Corporate Security team leader will assign the incident to an investigator; once assigned, the investigator will complete the following steps:

1. Conduct an in-depth interview of the initial caller for the narrative section of the interview report (who, what, where, and when).
2. Conduct any immediate investigative steps. For example, the interview of the initial caller may produce information not available to the responding police officer (i.e., the caller remembers there was a car that was suspicious the day before the break-in and wrote the plate number on his clipboard).
3. Enter the information in the relevant database.
4. Analyze prior thefts/break-ins for any similarities that may assist in developing a pattern of criminal activity that may assist in proactive steps to address future thefts/break-ins.
5. If patterns are developed, document the patterns and methodology determining the patterns in an e-mail to the Corporate Security distribution list.
6. At least quarterly, but whenever deemed necessary, GIS [geographical information system] mapping of thefts/break-ins should be compiled to map thefts/break-ins.
7. Continue to monitor the incidents for similarities and document any follow-up investigation. Ensure you clear security incidents upon arrest or admissions of subjects.
8. Save a copy of all assigned incident report forms to the t:drive/2012 Folder/Administrative/Incident Reports.

The Corporate Security team leader or designee will complete the following tasks:

1. Assign appropriate incidents for investigation by e-mailing the incident report form to the investigator for follow-up. Save a copy on all unassigned incident report forms to the t:drive/2012 Folder/Administrative/Incident Reports.
2. Ensure company executive management is briefed on any identified patterns of thefts/break-ins and preventive measures deployed to protect company assets and personnel.

ITEBOOKS.DIRECTORY

3. Review theft/break-in incidents with the entire Corporate Security staff at monthly meetings and ensure all personnel are current on criminal patterns and preventive measures being utilized by Corporate Security. Also, encourage input from all Corporate Security team members regarding this critical aspect of our core Security missions.
4. Coordinate investigative efforts throughout departments with cooperation and efforts of Security personnel.

The following memo was developed to ensure we had the support of the company's Legal Department:

Legal Opinion Regarding the Tracking of Copper Theft Subjects/Suspects

In 01/2012 and throughout 2012, Corporate Security began meeting the first Friday of each month to analyze incidents from the prior month and develop measures to address any issues from the prior month.

As part of this initiative, Corporate Security has initiated and maintained three separate spreadsheets: one to track the names of known copper theft subjects and suspects, another with a list of scrap dealers with a tiered system to track the most nefarious, and a separate list of law enforcement officials investigating copper thefts. The purpose of gathering and tracking this information was to maintain a list of persons known to have engaged in copper thefts through past law enforcement contacts and/or arrests, convictions, or past associations with criminal activity and to provide these data to law enforcement when patterns of criminal activity develop in their jurisdictions. The information is provided to law enforcement for whatever action is deemed appropriate and intelligence purposes as many of the subjects/suspects are repeat offenders.

In 01/2013, this information was shared with other utility Security managers, along with a concept to utilize the company extranet site as a central repository to share similar types of data throughout the utility industries and law enforcement community. During the meeting, a question arose as to the legality of tracking such information.

The Security team leader raised this question to the company deputy general counsel, explaining the information tracked by Corporate Security on the subjects/suspects was based upon open-source reporting or information from law enforcement. Upon consultation with others in the company's Legal Department, the deputy general counsel contacted the team leader and stated that the legal opinion was that this information may be tracked, utilized, and shared by Corporate Security with law enforcement and other security departments in the manner specified.

ITEBOOKS.DIRECTORY

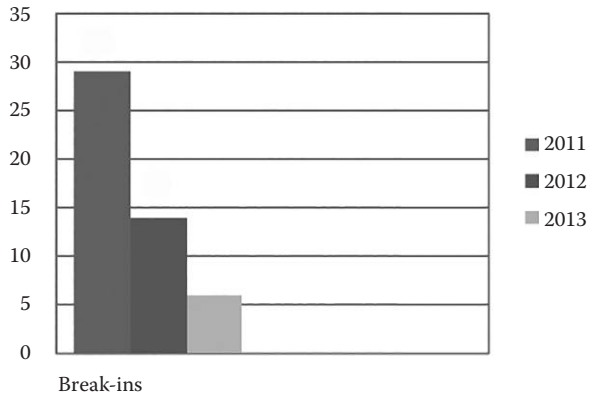

Figure 9.2 The company has experienced significant reduction in substation break-ins.

The results of our initiatives were rewarding. In 2011, we had 29 substation break-ins, and by 2012, we reduced the amount to 14. The number of substation break-ins was further reduced to 6 in 2013 (Figure 9.2).

Most satisfying was the success we had with law enforcement, with several of the thieves caught from the intelligence that we provided these agencies. The relationships with these detectives went from regular liaison contacts to real two-way personal relationships; they would go the extra mile for us because we had done so for them.

ITEBOOKS.DIRECTORY

10

Engage Executive Management

Depending on the size of your organization, security may be integrated within the legal, facilities, human resources, safety, or business services unit. The Security leader must have an understanding of the chain of command and the executives' view of the priority of security. The need for improvements in a security program or the initiation of an intelligence program may not be the priority of the Human Resources director and can be terminated prior to any presentation to any other company executives. It is imperative the Security leader engage his or her immediate supervisor to garner support for the security and intelligence programs. The improvements in the security program are generally encouraged and supported because they are perceived as part of the Security leader's job and within the scope of this position. Defining missions; writing policies, procedures, and processes; evaluating staff members; and collaborating with other departments are usually in the job description for this position when the person is hired. Recently, there has been a trend to add risk-based analysis of threats, and conducting assessments has been creeping into the Security manager job descriptions; however, the methodology or even value of these tools is not easily explained to the Legal, Facilities, Human Resources, Safety, or Business Services unit directors.

As you improve security operations and develop the security program, you should get a good read on the level of support you are receiving from your direct supervisor and executive management. If they are supportive, as you are developing the security program, look for areas that show some level of success by implementing an assessment methodology in the improvement of your security program that ties directly to areas of intelligence. For example, if one of your primary security missions is asset

ITEBOOKS.DIRECTORY

protection, assess and evaluate any criminal activity that has occurred against your company in the last five years. Sort the criminal activity into internal and external threats and concentrate your efforts on an avenue of reoccurring criminal activity. Examine the criminal activity for patterns and methods of operation; see if the offenders have been identified; look for patterns in time of day, month, or location; and meet with local law enforcement to establish contacts and to share information. The best way to develop valuable liaison contacts with law enforcement is to share information openly and candidly. The best way to alienate law enforcement is to ask for information but do not share anything you have and they find out later you were not forthcoming with them. Be honest and up front with them; generally, they will be the same with you. Of course, there will always be the exception, but most of those in law enforcement do want to make a difference and "protect and serve."

By integrating some intelligence program methodology in the security program assessment, you can develop engagement with your management chain and begin the education process to show them the value of the intelligence-based security initiatives. The point is to ensure that as you are conducting the assessments; if you are newer to the company, make sure you are engaging your management and understand their departmental and personal missions, objectives, and priorities.

Also, a painful reality is that just as important as it is to learn the daily operations, the official objectives, and overt company structure, it is imperative that you develop an understanding of the inner company politics. Knowing which manager, director, vice president, and president is involved in active feuds with other executives in your company is crucial information for survival of your programs. Awareness of the political landscape and the culture of your company is critical information and can play a major role in your strategic plan. Even the most brilliant of security or intelligence programs could be doomed if you stumble in the political arena of your own company.

Equally important for presentation to management is development of an executive briefing paper that synopsizes the security or intelligence assessments. Make sure the overall assessment is available if the individuals have time to read it or wish to utilize it as a reference, but a 50-page assessment must be reduced to 3 to 5 pages in a summary for ease of absorption and understanding.

Prepare and present the paperwork along with a brief PowerPoint presentation and allow the executives the time to ask questions. Have your subject matter experts in the room to answer any questions they may

ITEBOOKS.DIRECTORY

have; if you do not know the answer, tell them you will find out and follow up with them. Utilize any one-on-one face time with them to further your programs with a one- or two-minute "elevator" conversation. This means that, in the time it takes to ride on an elevator with an executive, you brief them with meaningful bullet points that will stick with them and sell your program. You are competing with company programs across your enterprise, and unless you had a significant security incident in recent memory, the executives will not have security on their mind unless you put it there with honest, realistic conversations.

At the two private companies where I worked since leaving the Federal Bureau of Investigation, I found there were different levels of engagement from management, but both companies' management did not understand what intelligence was or how it could assist the company in risk reduction. It took some work initially to educate management; the education phase did include examples of vulnerabilities or external threats that existed on site but was not documented, tracked, or analyzed. It did not take long to walk a site, talk to people who had been there a while, and identify vulnerabilities or threats that could be analyzed and documented and bring some familiarity to the intelligence presentations. It is impactful when you have assets that they see every day brought to them in a different light. It is the objective of any intelligence program to inform and ensure the company is aware of the risk. Knocking out the electrical power to a major 80-building campus and shutting down computer networks, security systems, lights, HVAC (heating, ventilation, and air-conditioning) systems, and plant operations for an extended period, say two weeks, by taking out one set of outdoor electrical panels is an excellent method of attack for the disgruntled insider or the insidious external threat.

So, meet with your facility's electrical engineer and conduct a vulnerability assessment of your electrical feeds from the municipality power company, walk the campus with your electrician, map and photograph the substations, and assess the critical electrical feeds. If an adversary takes out any one panel, does it affect the entire campus? If so, who knows about it? Everyone? Is there any access control? Is this a high insider threat vulnerability? How about weather? Could the panels remain intact in a tornado? How about an accident? Are the panels on a public roadway? If so, are they protected by concrete barriers? What kind of fencing is present? Write everything you find and, if there is a need for additional security measures, make recommendations. Put together a PowerPoint presentation and engage top executives (Figures 10.1 and 10.2).

ITEBOOKS.DIRECTORY

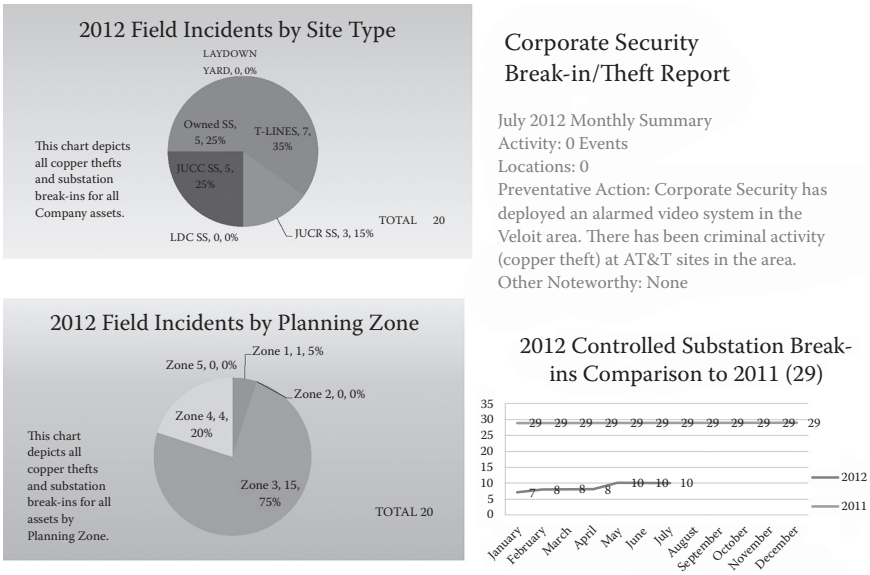

Figure 10.1 Incidents for 2012. JUCC—Joint Utility Control Common; JUCR—Joint Utility Control Retained; LDC—Local Distribution Company; SS—Sunstation.

ITEBOOKS.DIRECTORY

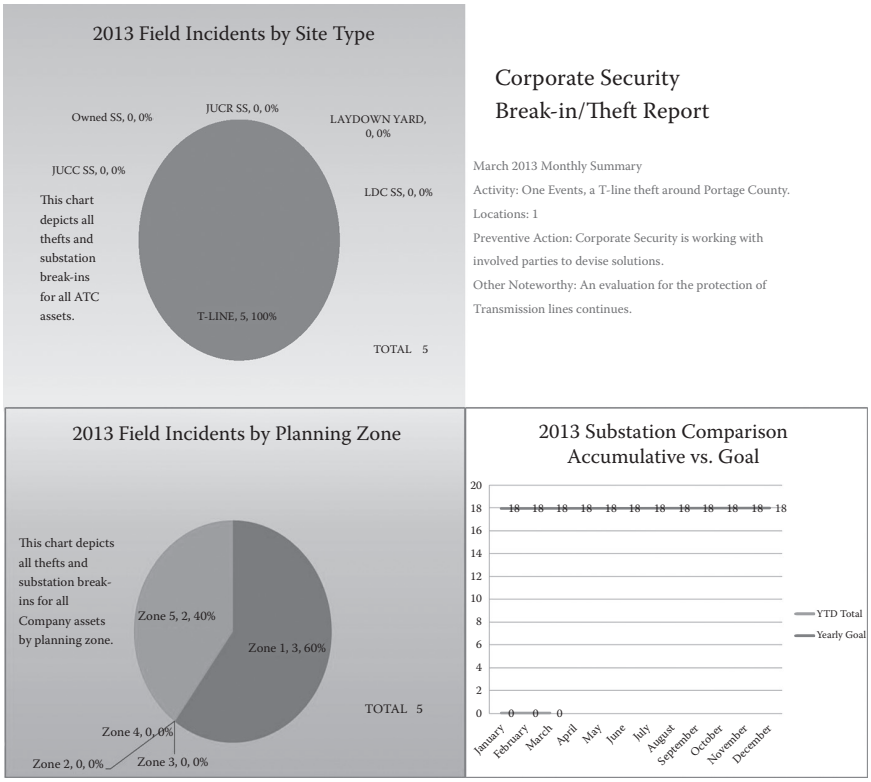

Figure 10.2 Incidents for 2013.

ITEBOOKS.DIRECTORY

ITEBOOKS.DIRECTORY

Section IV

Planning an Enterprise-Wide Assessment

ITEBOOKS.DIRECTORY

ITEBOOKS.DIRECTORY

11

External Threats

Intelligence Gathering begins with examining past incidents and past adversaries and the methods for causing harm to your organization. Within your organization, identify departments that have regular interaction with the public while carrying out their regular duties. The next step of our intelligence analysis revealed the utility company did not have a comprehensive security program to track persons who made direct threats to the company or its assets. The company built transmission lines by paying a "right-of-way" stipend to landowners; it had a vibrant community outreach program, with the mantra to "get people to like us." Several departments had contact with the public, and all of them kept a separate accounting of "problem" people, with no central repository or analytical lead.

Let me be clear that anyone has the right to express unhappiness with what they see as an unfair situation; however, when they make statements regarding physical harm to the company or its assets, these people have crossed a line. It is the duty of the security program to track these persons and make employees aware of the persons and the nature of their threats.

This led to awareness in different departments that a person had made threatening remarks without these departments informing others who would come into contact with this same person during the normal course of their employment. For example, if direct threats to harm company personnel were made at an open house, Customer Relations did not share the threat information with Construction, which built the lines on this person's property; Asset Management, which maintained the equipment; or Vegetation Management, which would trim the trees along the

ITEBOOKS.DIRECTORY

line, including this person's property. The potential for company personnel walking into a threatening situation unaware and unprepared existed.

To address the problem, an enterprise-wide assessment of persons who made direct threats to the company was conducted across all departments. The Security Department took the lead and became the clearinghouse for threat information. The people who made these specific threats were measured for capabilities to cause harm, and awareness flyers were made available to the entire company with available data and photos.

The specifics of what we did, as suggestions for others interested in this approach, included developing questionnaires eliciting information for incidents that occurred and caused concern for employee safety/security. These incidents generally occur within these groups through face-to-face interactions, phone calls, or e-mails or letters that contain some type of concerning communication expressing dissatisfaction with your organization. During your initial assessment, determine if these departments have recorded these concerns in separate internal databases; if not, obtain the information and develop a plan for the future. In an effort to address the identified risks and vulnerabilities, develop a central depository of external threat information that will be maintained by your Security Department or other appropriate department. As the information is received, Security will vet that information, evaluate the threat, and make a determination regarding the level of risk the threat holds for the organization. Security will then disseminate the information to the appropriate departments in an effort to protect the organization's assets.

Assess Threats—External Threats must define who. Who is the adversary? Who in the past, present, or future has posed or will pose risk for your organization by their intent to harm your assets? Are they capable of doing so?

A good example is a person showing up in the lobby of your headquarters demanding to see the chief executive officer. This person has every right to peacefully express disdain for your organization; however, the person becomes an external threat that should be investigated and tracked if harm to personnel or assets is threatened. In this situation, this person has clearly demonstrated intent; you need to investigate if the person can develop or already possesses the capability for a physical or cyberattack.

Along the same lines, presence and capability do not equal intent. Ensure you have a good handle on the threats in your arena and be able to assess their intent. This cannot be emphasized enough. A threat that is presented by someone highly capable of an attack can develop into an intent to attack your organization in the blink of an eye. However, a threat

ITEBOOKS.DIRECTORY

by someone with high intent and low capability will need time so the person can develop the capability to cause real damage. So, develop tools to monitor the intent and capability of known threats. Do not become complacent as intelligence threats are ever evolving.

Of course, there are instances when you may have a crime problem and cannot initially identify any subjects to evaluate. In the following example, over a decade there were several damaging incidents caused by local citizens shooting firearms in the vicinity of company transmission lines just outside Marquette, Michigan. In 2012, the company Transmission Line Maintenance Department had a meeting to discuss the matter. This meeting was attended by members of Asset Maintenance, Security, and Customer Relations Departments. After the meeting, Security took the initial lead on this project and, with collaboration with the group, developed an action plan.

> The first step of the security action plan was to gather intelligence, analyze available paperwork, and document past incidents. Investigation showed there was no security incident report regarding these incidents. Contact with local law enforcement did not yield any reports regarding any past incidents of transmission line vandalism. To track the history of incidents, Security conducted an analysis from maintenance records of documented incidents of vandalism provided by the company's Transmission Line Maintenance Department. The analysis showed 12 incidents of shooting vandalism in the period 2006–2012. After the initial analysis, Security made contact with law enforcement in the area, including the Federal Bureau of Investigation (FBI), the Michigan State Police, and the Marquette County Sheriff's Office. These contacts were made aware of the vandalism and agreed to a meeting to discuss law enforcement options with Security.
>
> Security and the transmission line maintenance engineer met with Marquette County sheriffs in Marquette to discuss options regarding transmission line firearm vandalism. Security then discussed the analysis with law enforcement and developed patterns (day of the week and time of day) of frequency of activity in the area. The detective from the Sheriff's Department stated there had been recent complaints of shooting the power lines in the area. Analysis narrowed the time of greatest activity in the area from 3 to 8 p.m. during the week and at any time on the weekends. The area was patrolled periodically and on a random basis by the Marquette County Sheriff's deputies. During the meeting, the detective stated his department had developed a camera with long-range identification capabilities. Security did not possess equivalent camera technology; this system

ITEBOOKS.DIRECTORY

has the capability to obtain quality photographs, including the ability to read license plates at approximately 300 yards.

The Sheriff's detective deployed his department's enhanced camera in the area of past transmission line firearm vandalisms. The police monitored this camera and were prepared to utilize any footage as evidence in the investigations of any crimes committed against the transmission lines. Also, the deputies did respond and speak to several persons they identified as shooting in the area. This put people on alert that law enforcement was aware of this activity.

The team evaluated existing laws concerning the criminal activity and researched what tools (laws) were available to law enforcement to address this issue. The Sheriff's detective provided documentation on two Michigan laws that applied to the situation; both were related to felonies that brought a five-year sentence on conviction. Information on the laws were sent to the company's Legal Department, which conducted additional research across the company's footprint and defined laws applicable to this problem. These laws were used to provide law enforcement with tools to charge offenders with felonies for damaging the power lines. These laws also allowed Security avenues to develop specific signage and the capability for a viable reward program. Signs were developed in conjunction with the Legal Department and deployed in the area of previous vandalism.

The team evaluated prior, existing, or future public awareness campaigns utilized to educate the public on the dangers associated with downed transmission lines (Figures 11.1 and 11.2). In July 2012, Customer Relations developed a press release and followed up with a comprehensive public awareness campaign, which included television coverage of the problem.

These strategies were deployed, and some, like the public awareness campaign, were updated prior to deer hunting season in Fall 2013. To date, there has not been additional damage due to shootings in the area.

Along with specific threats against your organization, analysis must be completed to evaluate threats against your industry. As attacks against companies similar to yours occurred in the past, they require evaluation. Are you prepared to handle a similar attack?

The next possible threats on the list to evaluate and assess were those from regional, national, and international criminal, terrorist, and extremist groups with a presence in our area of operations. We found there was a vast amount of data on the Internet that allowed us to educate ourselves on groups in our area, such as sovereign citizens, militia extremists, white supremacy extremists, ecoterrorist/animal extremists, anarchists, lone

ITEBOOKS.DIRECTORY

Figure 11.1 Upper Peninsula of Michigan transmission lines.

Figure 11.2 Another view of transmission lines.

ITEBOOKS.DIRECTORY

wolf/rogue offenders, and Al-Shabaab (international terrorism). The websites of the FBI, Department of Homeland Security (DHS), and National Counterterrorism Center were also valuable for background information. Liaisons with federal, state, and local law enforcement were also valuable tools for this section of the assessment. After obtaining background on each of the groups, we addressed three areas; the following on Al-Shabaab is an example:

Presence in Company Footprint: Al-Shabaab will have a presence in any metropolitan area where there is a Somali population; there is a documented presence in Minneapolis, Minnesota, and parts of western Wisconsin. Al-Shabaab members are easily within driving distance of any company assets they decide to target.

Capability: Al-Shabaab has deployed American citizens from Minneapolis to Pakistan and the Middle East to join the jihad (holy war) against enemies of Islam. They have also employed mass murder, as demonstrated in the Kenya mall shooting detailed in news reporting.

Intent to Harm the Company/Utilities: To date, specific threats emanating from Al-Shabaab to the company have not been uncovered; however, open-source reporting indicates there have been attacks on the electrical utility industry overseas. As Al-Shabaab has a presence in the company's footprint and past attacks have demonstrated the capability to plan and execute violent attacks when provoked, the group should be included in any future company asset risk/threat assessment. Their intent should be monitored.

These organizations with a presence in your enterprise footprint should be evaluated regarding capabilities and a method set up to measure their intent regarding attacks on your industry or specifically your organization. The benefits of gathering, analyzing, and acting on actionable intelligence can become quickly apparent by concentrating resources on your most prolific crime problem. For example, if you begin to track perpetrators of criminal activity targeting your organization, the likelihood of identifying repeat offenders is high. Criminals are people, and people tend to follow familiar patterns in any profession. Simply stated, bank robbers rob banks, credit card thieves conduct identity theft, burglars break into properties, embezzlers steal funds, and so on.

As we learned with the substation break-ins/copper theft initiative, identify any criminal activity that has been common to your organization in the last five years and obtain police reports on all of the activity; analyze

ITEBOOKS.DIRECTORY

the material for patterns and common offenders. Once you have identified the offenders, utilize social media and open-source reporting to determine their "support group" or organization. Identify geographic areas of operations and methods of criminal activity. Share the results of your analysis with local law enforcement. Ensure you share the information with local law enforcement at the detective level; the detectives generally are the "intelligence officers" in local police departments. Monitor criminal activity, and when the next "spike" occurs, recontact these detectives to share the names of the identified subjects for their investigative purposes. They will contact the known offenders and either build a case against them or make them informants to address the crime problem. The fact that the police are questioning criminals who had been convicted in the past will "get the word out on the street" and have a positive effect in reducing the criminal activity. No criminal wants go to jail; the higher the risk of incarceration, the less likely the criminal activity will continue.

Develop liaison networks in your industry, law enforcement, intel agencies such as the DHS/FBI, fusion centers, corporate departments, and contractors. The more personal the developed contacts are at each level, the more likely there will be results from any requests. Ensure the assessment of any threats (groups and persons) includes open-source reporting and the exploration of social media.

Develop and utilize an assessment methodology specific to your identified objectives for security in your organization. As stated previously, reviewing, organizing, tracking, and documenting past incidents that have occurred not only in relation to your organization but also to other organizations in your industry will be the base of the assessment process. The saying that "those who don't learn from history are destined to repeat it" applies to organizations that do not have a formal system set up to track significant security events. Those who do not track events of the past and as they occur find themselves handling each event as a new problem and as a crisis, often committing many of the same mistakes in resolving the situation. If these events are familiar and standard operating procedures are developed to address them that are specific and fact based, resolution will be more effective, efficient, and repeatable.

ITEBOOKS.DIRECTORY

ITEBOOKS.DIRECTORY

12

Industry Threats

Any industry will have vulnerabilities and threats that are generic to the line of work in which they engage. For example, the food industry must evaluate and assess the possibility that someone may taint or poison products. Whether you are evaluating an insider or external threat, the vulnerability remains constant across the industry. Discussing vulnerabilities with subject matter experts within your industry is highly recommended. The development of an extensive network of industry contacts can be accomplished by leveraging professional networks specific to your industry, such as national associations, regional groups, and even social networking. Social networking sites such as LinkedIn have group discussions specific to industries.

Subscribing to magazines and websites and developing e-mail alerts and twitter feeds from industry-specific sites can assist in maintaining the pulse of threat streams of interest in your industry. Forming collaborative working groups that meet even through e-mail contacts to discuss these threat streams is critical to allow your intelligence and security programs the flexibility to evolve with threats as they change. Always remember the "bad guys" are constantly assessing us and what systems and protections we have in place to defeat our security measures and harm our assets, people, and reputations. Knowing who your adversaries are and how they operate is a battle that is constantly waged. Waves of criminal activity can be prevented if law enforcement, intelligence agencies, and security departments identify trends and quickly adapt to place appropriate security countermeasures throughout an industry to address the new threat.

ITEBOOKS.DIRECTORY

One of the groups that I personally initiated was the former Federal Bureau of Investigation (FBI) Agent Electrical Utility Group; there were many of us who had retired from the FBI and gravitated to security jobs in the electrical utility industry. One commonality we had was a like way of thinking from our bureau backgrounds. Many of the executives in the electrical utility industry were engineers, who also thought in similar ways, but the levels of communication with their security departments were at times taxing to both engineers and former FBI agents. The working group exchanged ideas and incidents through e-mails and conference calls. I found it helpful and invigorating that I could "speak to my own kind" about security and electrical industry issues with clear understanding.

We also met regionally with other members of the electrical utility industry and exchanged best practices and threat information. We scheduled regional meetings on a quarterly basis unless a significant issue arose. The amount of intelligence generated from such collaborative groups is extremely valuable, as shown by the incident described next. The sharing of information regarding significant events through industry networks allows you to assess, evaluate, track, and prepare for similar attacks.

With strategies in place to evaluate threats, we were prepared when the Metcalf California substation shooting took place in April 2013. Even though it was thousands of miles away, it was an attack on our industry, and we were prepared to address a similar matter. The incident in which a physical attack (shooting) of an electric utility substation in suspected conjunction with a physical attack on telecommunication cables (they were cut) defined a need to assess the vulnerabilities that may exist at our company regarding this threat stream. With the Security Department taking the lead role, we convened a working group that accomplished the following tasks:

2013 California Incidents

Substation Threat Reporting, Tracking, and Analysis

Overview/Mission

A physical attack of an electric utility in apparent/suspected conjunction with a physical attack on AT&T telecommunication cables has defined a need to assess the vulnerabilities that may exist at the company regarding this threat stream. Therefore, with Corporate Security taking the lead role, the company will convene a working group to accomplish the following tasks:

ITEBOOKS.DIRECTORY

1. Review the California incident
2. Assess vulnerabilities
3. Review current practices and our preparedness
4. Develop an action plan

Working group members include representatives from Corporate Security, Critical Infrastructure Program (CIP) Office, Emergency Management Systems, Asset Maintenance, Communications, System Protection, Asset Performance, Metering and Control, and Information Technology Security.

Incident

Information received from a bulletin dated April 18, 2013, was that on Tuesday, April 16, 2013, vandalism in the form of multiple gunshots at a large substation in the Silicon Valley area resulted in substantial equipment damage. Fiber communications lines were cut prior to the substation damage, disabling data flow and 911 call capability. The attacks marked an increased level of scale and sophistication in vandalism to energy and communication infrastructures.

Information received from the victim company was as follows:

Fiber-optic and copper cables cut.
Six fiber cables cut in one vault, another data cable cut in a second vault.
Fiber cable cut in a way to prevent repair. Individual had knowledge.
911 communication impact: Law enforcement believes the purpose of cutting cable was to delay law enforcement response, not impact SCADA [supervisory control and data acquisition] operations.
SCADA communications were not affected.
Substation came under gunfire.
150 rounds of 5.56-mm shells found in vegetated area 20–40 yards from substation fence line. Chain link fence was not penetrated.
Very accurate shots in low lighting. Shooters probably used some type of night scopes.
Suspect one or two shooters involved.

Facts

The following facts have been gathered to date: On Tuesday April 16, 2013, at approximately 1:00 a.m., AT&T had fiber-optic and copper cabling cut at a site in Gilroy, California. This action disrupted Internet, wireless, and landline phone service in Santa Clara County, California. News reporting stated there was a similar incident in April 2009; vandals cut

ITEBOOKS.DIRECTORY

cables in south San Jose, California, which caused telecom disruptions in Santa Clara and Santa Cruz counties.

On the same date, about a half mile from the AT&T affected resources, the victim company substation was riddled with rifle gunfire around 1:30 a.m., leading to the speculation the incidents were linked. The extent of the damage was outlined in the victim company news conference highlighted previously.

Possible Threats

Based on the available information, the following theories may apply to the suspects:

- Random act of vandalism.
- Possible insider threat since there have been two AT&T incidents in the last four years; it is possible the substation attack could have been to cover the AT&T vandalism. Suspect could also be PG&E [Pacific Gas and Electric] insider.
- Both incidents could be a test of incident response by either criminal or terrorist elements. This could also be a trial run of a physical attack on critical infrastructure resources.

Company Issues/Vulnerabilities

The significant vulnerabilities of the company were assessed and listed. To list them would put the company at risk.

Current Security Posture

Within the last 18 months, to address the past issues in Corporate Security, current leadership established and focused on the three core missions: asset protection, compliance/training, and physical access control.

Throughout 2012, the day-to-day operations of Corporate Security have improved, and the continuous improvement continues in 2013. As daily operations stabilize, Corporate Security has expanded into areas not previously addressed. New Corporate Security initiatives tied directly to this issue are as follows:

- Introduction of intelligence-based security initiatives.
- Close coordination with Cyber Security.
- Close coordination with Asset Maintenance and other departments regarding the shooting incidents in Marquette County, Michigan.
- Coordination with Substation Standards to define universal door, crash bar, and entrance points and a physical security risk assessment on any new substation construction.

ITEBOOKS.DIRECTORY

Figure 12.1 Transformer.

- Physical security risk assessments for substations and new construction projects that include demographics and crime statistics and examine past criminal activity to measure vulnerabilities to physical attacks (Figure 12.1).
- Initiation of the External Threats Working Group to consolidate information on threats from outside the company's enterprise.
- Initiation of the Insider Threats Working Group to evaluate and mitigate threats that may affect/emanate from personnel and contractors.
- Reduction of traditional copper thefts/substation break-ins (29 in 2011 and 14 in 2012) through intelligence gathering of criminal intelligence, spreadsheets of the names of known copper thieves, liaison with detectives specializing in copper theft, and nefarious scrap yards. Close coordination with Asset Maintenance and Construction regarding copper thefts.
- Utilization of GIS [geographic information system] data for threat and theft tracking.
- Increased liaison with other utility security and local law enforcement.
- Constant evaluation, expansion, and deployment of the technical capabilities of security equipment, video systems, high-resolution cameras, and intrusion detection devices.

ITEBOOKS.DIRECTORY

Action Plan

Upon conclusion of the initial meeting, it was decided the following measures would be recommended:

- Continue with the evolution of the security strategy to an intelligence-based security posture, including engagement with Cyber Security and groups across the enterprise.
- Develop an incident response/crisis management team to handle incidents as they occur throughout the company's footprint.
- Develop an incident communications process to notify and engage appropriate personnel in relation to incidents.
- Appropriate departments should conduct an assessment of the equipment critical to bulk electric system operations in substations for any specific physical attack vulnerabilities.
- Appropriate departments should determine what risk assessments are being done by personnel/departments, including projects such as the Minimum Visibility Substations (MVSs) assessment to determine/prioritize substation communications and other efforts, to share appropriately.
- Corporate Security and Asset Maintenance will consult with Legal to determine if signage should be displayed on substations with specific language to laws and penalties for damages to substations.
- Corporate Security will ensure any substation break-ins and/or significant incidents are reported to the appropriate Systems Operations Centers for situational awareness for responding personnel.
- Corporate Security and Asset Maintenance will continue to conduct an assessment of substations.
- Fund and staff a corporate security command post (in-house 24/7 security alarm monitoring) under a one-year pilot project.
- Corporate Security requires an additional security technical specialist; the position has been funded for 2013. A review of the position and need drives are being completed.
- Consider hiring an intelligence analyst to analyze, prioritize and document threats to the company.
- Continue to coordinate with security departments of like industry partners in sharing potential action items regarding this and other common threats.
- Continue to coordinate with the FBI/Department of Homeland Security (DHS) and law enforcement regarding this incident and other pertinent threat streams.

ITEBOOKS.DIRECTORY

Arkansas Incidents

Summary

Information received from a telephone call on October 2, 2013, was that on August 21, 2013, vandalism in the form of the damaging of a 500-kV transmission tower in rural Arkansas resulted in substantial equipment damage. On September 29, 2013, a substation with four 500-kV lines was broken into, and the substation control house was intentionally ignited and destroyed by fire. This incident was within 10 miles of the transmission tower incident on August 21, 2013.

Information received from the victim company representatives on the October 2, 2013, telephone call was:

Transmission Line

In the early morning hours of August 21, 2013, in rural Arkansas, located in western Lonoke County, a 500-kV transmission line lattice metal structure was found to be damaged as a Union Pacific Railroad train cut through a conductor on the railroad tracks. The conductor came from the damaged transmission line structure. Further investigation revealed Union Pacific reported they had noticed a "line" across the railroad tracks approximately two weeks before the August 21, 2013 incident. (It was not clear from the telephone call if this was discovered through investigating the August 21, 2013, incident or reported prior to the discovery of the damaged transmission line.)

Investigators found that unknown subjects had fastened a cable to the transmission line metal structure, then placed it across the railroad tracks and fastened the other end to a tree. When this did not take the transmission tower down, it appears the unknown subjects loosened bolts in the transmission line structure and strategically cut the tower to drop the conductor across the railroad tracks. It was reported a passing train cut the conductor in half and dropped the line across a neighboring highway. Other items of evidence include duct tape found on the scene and sections of rubber garden hose that was used to encase the cable prior to it being draped across the railroad tracks.

Substation Attack

The second incident on September 29, 2013, was the fire at the 500-kV substation at a location reported to be within 10 miles of the transmission tower incident. The information from the alarm log was that at 4:32 a.m. an intrusion alarm from the control house was received, at 4:36 a.m. the first of the trouble alarms was received from the substation control

ITEBOOKS.DIRECTORY

house. By 4:37 a.m., the first of four transmission lines was tripped. The victim company dispatched first responders and the Lonoke County Sheriff's Office; they arrived at approximately 5:30 a.m.

Further investigation revealed the unknown subjects cut the locks off the substation gate to gain entry. They proceeded to the control house and cut a padlock off the door to gain entry but set off a contact intrusion alarm. The subjects did not appear to directly physically attack the equipment in the control house, with the exception of starting the fire. There was a motion-detecting camera alarm system, but it was not aimed at the control house but behind the control house, pointing at the substation equipment in the yard, to protect against copper thefts. The motion alarms were never triggered.

Status of Investigation

The FBI, ATF [Bureau of Alcohol, Tobacco, Firearms, and Explosives], and local law enforcement have been involved in the investigation. The following were the highlights:

- Investigating logical suspects with vendetta against victim company (external threats).
- Investigating logical insider threats (items left behind may indicate insider).
- FBI is aware of two antigovernment groups in the area, checking for any ties to the incidents.
- Investigation has led to some "persons of interest" but no solid subjects.

Action Plan

- The long-range strategy includes the substation "hardening" initiative, which is a collaborative effort to level physical security at the company's most critical substations for resiliency.
- Continue to monitor and evaluate external threats.
- Continue to monitor and evaluate insider threats through the Insider Threat Working Group.
- Conduct a GIS assessment of railroad lines within 50 yards of transmission assets for situational awareness.
- Contact Union Pacific Railroad Security and develop appropriate liaison contacts to share information for future threat intelligence.
- Maintain liaison with local FBI officials to share information for future threat intelligence.
- Assess history of control house fires in the footprint for any value.

ITEBOOKS.DIRECTORY

As we had been addressing issues such as the substation break-ins, copper theft, and shootings on our sites, when these industry threats took shape across the country, we were in a position to quickly analyze company vulnerabilities and make recommendations to minimize risk in the threat vectors as reported. We also had law enforcement, industry partners, and other company departments engaged in the prior projects, such as substation break-ins, and it was easy to engage them in the new threats. Building and maintaining the relationships through meaningful engagement such as working together on projects that are successful is true team building that can be applied to future projects. It was rewarding to do so when the California and Arkansas incidents occurred. We were able to move quickly and efficiently.

ITEBOOKS.DIRECTORY

ITEBOOKS.DIRECTORY

13

Internal Threats

As damaging as attacks from threats outside your organization may be, an attack by a person who works for you and who has designed the very systems that keep you safe is far more ominous. Some of the most significant and notorious figures in American history have caused insider threats. These individuals include Benedict Arnold in the Revolutionary War; Tokyo Rose in World War II; Julius Rosenberg, who sold the atomic bomb to the Soviet Union; Robert Hanssen, the Federal Bureau of Investigation (FBI) agent who spied for the Soviet Union; John Walker Jr., the U.S. Navy communications officer who spied for the Soviet Union; and Aldrich Ames, the Central Intelligence Agency (CIA) analyst who also spied for the Soviet Union. Today, these figures include Nidal Malik Hasan, the U.S. Army major who murdered 13 people at Fort Hood, Killeen, Texas; and Adam Yahiye Gadahn, also known as Azzam the American, who worked for Al Qaeda. Ames, Hasan, Walker, and Hanssen were trusted U.S. government employees; all had high-level U.S. government clearances, and all of them spied for the Soviet Union.

People are any organization's greatest asset; the engaged, hardworking, productive, and motivated employee drives a company's success. The person who has the "keys to the kingdom" as part of their job also has the capability to cause great damage to the company; the content employee poses no threat, and as long as this employee remains content, there is no problem. However, if that same employee has several negative life issues, say, for example, his wife leaves him, he starts drinking too much alcohol, and he develops some sketchy associations, and these are compounded by a new boss who got the promotion that the employee did not—the valued employee can develop the intent to harm the company and in essence

ITEBOOKS.DIRECTORY

becomes the toxic insider threat. This situation, if not detected and handled early on, can be the most devastating of threats. As in the examples of Ames, Walker, and Hanssen, an insider can operate undetected for years before finally making a mistake and being caught.

A trend to address workplace violence has recently brought this threat to the forefront of many corporate security departments. The impression is that active shooter incidents may be reduced by treating people with respect and avoiding key words such as *terminated* or *fired*, respectfully letting people go from their positions. Although there is much value in always treating people with respect and dignity, the underlying issues that cause an individual to pick up a rifle and go to work to kill people, most likely dying themselves, do not generally hinge on the method of how they were "let go." There are many other factors that must be considered and tracked, such as capability and intent.

A threat assessment of anyone who has risen to the level that their employer views them as a possible threat must be evaluated and the assessment be documented and tracked. A person with known developed capability, let us say a legally obtained arsenal that other employees have seen, can act quickly compared to a person who needs time to obtain the firearms and "practice" to become familiar with the weapons for their attack.

However, there are still many things that law enforcement and intelligence professionals do not understand; there have been incidents of subjects planning a shooting attack, had the weapons, did the homework on law enforcement response, written their grievances, and then committed suicide at their home. So, what makes them different from the Colorado movie shooter or Hasan at Fort Hood? It is hoped someone will figure out a formula to obtain help for people before they start down the dark pathway in the first place.

However, the point is that there is a corporate security focus on workplace violence that is concentrating on "active shooters"; the insider/internal threat brings many avenues of attacks that can cause damage. The threatening actions of corporate insiders include anything from disrupting the ranks with poisonous gossip to actually committing an act of sabotage (cybersabotage and physical sabotage), workplace violence (including as an active shooter), sale of trade secrets, theft, and general malfeasance. The program that is developed should find the root of the problem, and either bring the employee back into the fold or terminate the individual's employment. By the time they leave, the Security Department should have an assessment of the individual's capability to harm the company across the spectrum of threat streams.

ITEBOOKS.DIRECTORY

The goal of any company should be to assist the employee back to a level of normalized operations and reduced risk from the people in positions that if compromised could seriously damage the company. However, as Human Resources is "normalizing" the employee through counseling and employee assistance programs, the company should monitor the employee's critical access for any possible nefarious activity. In other words, Cyber and Physical Security should put "trip wires" in place on the employee's cyberaccounts; monitor the individual's social media accounts; and use any other legal means of monitoring while the employee stabilizes.

An insider threat is a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors, or business associates, who have inside information concerning the organization's confidential business information, computer systems, data, and physical and cybersecurity controls. Their capabilities may involve acts of fraud, the theft of confidential or commercially valuable information, the theft of intellectual property, damage to company assets, physical harm to personnel, or sabotage of computer systems. Employees and trusted contractors not only can be the organization's greatest asset but also can be the organization's greatest risk.

It is highly recommended that a collaborative group be formed in your organization. The group should consist of, but not be limited to, members of Security, Cyber Security, Human Resources, Legal, and Internal Audit Departments; it should initiate an assessment of the insider threat risk within your organization. These are the departments that we involved when we initiated the Insider Threat Group at the company where I worked. Security took the lead. At monthly meetings, the group coalesced; each department's views were heard and incorporated into the group's essence.

To elaborate, the importance of the collaborative group is related to the different perspectives each member brings to the table: the Security professional will evaluate any situation in an effort to reduce risk, the Human Resources member will ensure the rights of the individual member are protected to further an open and fair work environment, and the Legal member will ensure the organization is protected from any unnecessary lawsuits. If the working group members develop a working relationship that allows each of the member's viewpoints to be heard and trusts that each member is acting in the best interests of the organization, the working group will evolve into a valuable asset for your organization.

Be warned that the potential for abuse of the members of the Insider Threats Group is as real as the insider threats are themselves. The strength of forming a collaborative working group across several entities helps put

ITEBOOKS.DIRECTORY

checks and balances into place to prevent any group from becoming powerful enough to investigate, judge, and mitigate employees in the organization. The multifaceted approach will ensure a more impartial review of the facts of each individual case. Everyone has someone they do not like for some reason; there is danger in one group handling the Insider Threat Group and developing "personnel problems" related to people they do not like and using the insider threat excuse to clean house. Reporting to an executive-level oversight committee may help address this danger.

The initial insider assessment may concentrate on developing a capabilities matrix related specifically to positions within your organization. For example, what are the capabilities of the information technology manager in your organization, no matter who is in the position?

Eventually, you must expand the working group. The group must include the ability to evaluate individual situations (personal crisis) where organization personnel/contractors may cause them to develop malicious intent and monitor their activities/capabilities to potentially harm your organization or its affiliated until the situation is resolved.

The following material was developed regarding the insider threat program initiated at the utility company:

> Starting late in 2012, Corporate Security, Cyber Security, and Internal Audit convened and initiated an assessment of the insider threat risk at the company. The initial assessment concentrated on developing a capabilities matrix related to positions at the company. The assessment expanded to developing the ability of the team to evaluate situations where personnel/contractors may develop personal situations that could possibly devolve into malicious intent and monitor their activities/capabilities to potentially harm the company or the bulk electric system until the situation is resolved.
>
> The process of evaluating employees who came to the attention of Human Resources for whatever reason was handled in the past as an informal process. Human Resources would evaluate the situation, engage Legal and Corporate Security, develop a plan, and execute upon input from represented parties.
>
> On February 20, 2013, a meeting was convened to explain the mission to Legal and Human Resources Departments, elicit their opinions, and formalize past practices and to include them as participants in the Insider Threat Working Group.
>
> After discussions of the Insider Threat Working Group were concluded, Legal and Human Resources agreed to participate in future meetings. If an event occurs, Human Resources will discuss the matter with Legal. Human Resources and Legal will then convene the Insider

ITEBOOKS.DIRECTORY

> Threat Working Group and brief attending members to the necessary level (within Legal and Privacy limits) they will need to develop an appropriate proposal to address the situation.
>
> Based upon this collaborative effort, tailored to each specific situation, suitable levels of protection will be deployed to company assets. These measures will be monitored and maintained through the duration of the event. Once the employee stabilizes, the measures would be retracted, and all would return to normal. Discussions determined and documented a clear mission statement. "To diligently and discreetly assess and mitigate any/all possible threats, brought to the group's attention, which may emanate from or affect Company operations and assets, including personnel engaged in any capacity by the Company."

This formula worked for us, and our Insiders Threat Working Group was successful.

After the fact, in many attacks or crimes by insiders, you hear people say, "Well, I knew that was coming; he was always threatening people and nobody ever did anything." Employees have behavior traits, indicators of potential violence, or intents to commit an act against a company's assets or people; these are (but are not limited to) the following:

- Suicidal ideation: comments about "putting things in order"
- Behavior or statements that may indicate paranoia ("Everybody is against me")
- Increasing mentions of problems at home
- Escalation of domestic problems into the workplace; talk of severe financial problems
- Talk of previous incidents of violence
- Empathy with individuals committing violence
- Increase in unsolicited comments about firearms, other dangerous weapons, violent crimes
- Increased use of alcohol or illegal drugs
- Unexplained increase in absenteeism; vague physical complaints
- Noticeable decrease in attention to appearance, hygiene
- Depression/withdrawal
- Resistance, overreaction to changes in policy, procedures
- Repeated violations of company policies
- Increased severe mood swings

Education of any insider threat group is imperative and should include the potential indicators. In addition, as the group initiates and stabilizes, education should be extended to executives, managers, and eventually the

ITEBOOKS.DIRECTORY

general population. Give your employees an avenue to report abnormal behavior and develop a program that is fair to those who are reported.

Remember, the last thing you need is a "witch hunt" or employees using the insider threat group as a tool to "weed out" people whose only crime is they that "do not fit in."

ITEBOOKS.DIRECTORY

14

Vulnerabilities

The next critical assessment component is to measure your vulnerabilities, described previously as the evaluation of the organization's assets and determination of how susceptible those assets are to attack. As you evaluate the specific and general threats that have developed and the capability of those associated with the threats to attack you, evaluate your assets to determine how vulnerable your assets are to attack and document the findings (Figure 14.1). For example, chain-link fences and padlocks on a remote unmanned location without any means to receive or monitor alarms or any camera systems to view the location make the location more vulnerable than a manned site with analytic video camera systems monitored by a 24-hour central alarm station. The key questions for the vulnerability component are the following: What are we going to protect? How are we protected now? How would we attack us? How can risk to operations be minimized? Vulnerability assessments of critical assets cross from the human factor to include the possibility of harm from weather events or natural disasters. The critical asset must be looked at from every angle, human and natural, for protection.

As the security expert in your organization, know your limitations. If your organization has equipment or assets that you do not understand, ensure you enlist the aid of subject matter experts within your organization who maintain or design the equipment in the vulnerability assessment. They will know the equipment's vulnerabilities from industry experience; they will have methods to disable the equipment that can be utilized by an adversary, knowledge critical to your assessment. Engaging the facilities manager, safety manager, company engineers, and those

ITEBOOKS.DIRECTORY

Figure 14.1 Visually inspect for vulnerabilities.

responsible for the primary mission of your company will enable these individuals to tell you the vulnerabilities the company may be facing.

Assessing key departments and engaging their subject matter experts in a collaborative session to discuss vulnerabilities is a fascinating and enlightening project. When you explain the objectives of your vulnerability assessment and point out a simple vulnerability, the ball will start rolling so quickly you will not be able to write fast enough to document the information you will obtain.

A simple example is to look for any large amount of fuel oil or combustible material and evaluate the physical security measures protecting the vessel where it is stored. If the physical security measures need improvement or even if they do not, bring the assessment you completed at the first meeting with the subject matter experts. Assemble and present a PowerPoint presentation with photographs; provide an explanation of the vulnerability you assessed regarding the combustibles, your evaluation of the physical security measures along with the strengths and weaknesses of those measures, and any recommendations for improvements. Then, in an open forum write the most vulnerable items identified on a whiteboard or flip chart. Be prepared to hear such comments as, "Yeah, that is a good one, but if you take out all the electrical panels next to 41st Street you would shut down operations here for weeks and bring all of our operations to a standstill. The only thing protecting the panels is a chain-link fence."

ITEBOOKS.DIRECTORY

These subject matter experts know everything about your company, how it operates, and what would negatively affect company operations because they have lived their jobs for years in some instances. They read manuals on equipment; they go to seminars and talk to other subject matter experts, share experiences, and talk about and solve industry problems and issues. They are the most valuable assets your company has; engage them, allow them to assist you in identifying the "crown jewels" that your company must protect at all costs. Elicit their opinion on how best to protect the assets and develop contacts with them so in an emergency you know them and can obtain answers quickly. Also, know who they are because, as mentioned, if they develop intent to harm the company, they also will become the greatest threat to the company because of this knowledge. In reality, any intelligence-based assessment that does not include the subject matter experts within your enterprise would be a vanilla outline of the assessors' point of view.

Ensuring you engage the people that make the company run on a daily basis (e.g., the facilities personnel), not just the engineers, is also vital. The engineers think like engineers and think how things work in theory, but the people that ensure the daily operations are also valuable resources for interviewing to develop your assessment methodology.

Do not be an assessment snob and think that these people are "laborers" or are not a valuable source of information. They will know things about your facilities you would only find out by "being in the trenches" for many years. They will know what tunnels have access to any systems underground, when they were maintained, if there are any homeless persons who have set up camp in your facilities, and so on. The people who have been maintaining your facilities on a daily basis for decades will know every nail, screw, and bolt in your buildings. You will be amazed at the information you will obtain if you engage them in the assessment. Formulate some questions but be prepared to sit for a while; if you get them talking, they will be a wealth of knowledge.

During the interviews and engagement with the subject matter experts and facilities workers, ensure you ask how they know the information you are gathering and try to "vet" the critical assets that you identify with some technical documentation to ensure your assessment has factual backing and roots in legitimate vulnerabilities. Walk the areas with the people who provide you with vulnerabilities of critical assets and photograph the areas of concern. At the utility company, we were concerned about substations and implemented the following general plan for assessment and risk mitigation:

ITEBOOKS.DIRECTORY

Substation Hardening Initiative

Identify your critical/essential assets.
Conduct specific assessments for each critical/essential facility/asset.
Utilize the gathered intelligence and make recommendations to mitigate/reduce risk through collaborative programs with key departments.
Implement appropriate physical security devices and methods as determined by a risk assessment, such as, but not limited to, blast walls, no cut/no climb fencing, high-definition cameras, and infrared motion sensors.
Initiate a command post for incident/alarm to develop a process for response and restoration efforts for security events.

As we moved through the assessment phase at this company, we developed a specific collaborative working group to address hardening of all assets within the perimeter of our critical substations. The solutions were costly, and resources are always limited. Identifying critical assets, the ones that if you lose them your operations fail or grind to a complete halt, is harder than may initially be assumed; the identification must be documented for future reference and analysis.

Any loss of assets may affect a company's operations, but there are certain critical functional departments that are common to all of today's companies and what they need to operate; these functions are related to electric power, computer networks, communications networks, and people to run them. Start with them and expand the vulnerability assessment to specific operations of your company.

ITEBOOKS.DIRECTORY

Section V

Compiling the Assessment

ITEBOOKS.DIRECTORY

ITEBOOKS.DIRECTORY

15

Planning and Resources

With the alignment of your key stakeholder and critical liaison contacts in place and the mapping done on the critical components, internal threats, external threats, industry threats, and vulnerabilities specific to your company, it is time to tie them together to complete the overall enterprise assessment. If you have staff who have been assisting you with the components, it is time to bring them together and engage in the planning of the enterprise assessment.

A planning meeting to gather and evaluate the next steps in the final assessment will have to include members of each of the components; at this point, several programs will be assembled into a final product. The expertise developed in the evaluation of the programs these individuals were leading will now pay off in exponential dividends. The goals are to evaluate the connectivity of threats and to develop measures that ideally will reduce risk across several threat streams. This may provide cost savings to the company; if so, executive management should be briefed. Even if the assessments do not show immediate cost savings, brief executive management as this point in compiling all the intelligence components into one assessment is a major milestone in your company's intelligence program. If you engaged these individuals early in the process, they will be interested and supportive; if this is the first they are hearing about all the components, you must emphasize any success that you have attained from the initiatives that are intelligence related.

Assemble your intelligence subprogram team leaders, subject matter experts, key stakeholders, operations personnel, and liaison contacts and engage them in planning the enterprise assessment. Define the scope in stages and evaluate the priorities; establish timelines and formulate

ITEBOOKS.DIRECTORY

subteams for areas that may need more work than the clearly defined missions/objectives.

Some of the threat stream subprograms may be further along than others because of the strength of the teams, or duration of operation; it is hoped that the more established teams have reached maturation and are knowledgeable. The teams formed later or that are more complex may be in need of bolstering. Other teams may not have enough information to be clearly delineated in the initial enterprise assessment.

If the insider threat group is a collaborative effort of several departments, there may be a general overview of person-based capabilities that may not require a specific view in the enterprise-wide assessment. If you are preparing to address insider threats through a working group that has not been formed or has been discovered in an existing group (e.g., risk management has been addressing insider threats in your enterprise), that does not mean you do not include the analysis in the assessment. Engage any existing insider threat team and measure its capability: Is the team tracking existing and past threats? You do not need to identify that Joey Bananas in the mail room is a former Special Forces demolition expert who has come on the insider threat radar to begin to plan for an insider threat bombing scenario.

Tracking specific threats is invaluable because you have the advantage if you know someone capable of an attack may be developing intent; specific trip wires can be put into place. However, in planning an assessment and program, prepare for the entire scope of human-driven attacks. Plan and be ready; when your insider threat team matures, the team will be ready to execute premeditated plans.

Available sources for information in the analysis of external threats include the Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), other government websites specific to your Industry, Fusion Center contacts, law enforcement liaison contacts, companies with similar operations that form regional collaborative groups, open-source reporting, general social media, adversary websites, social media sites, public judicial websites, county real estate records, probation and parole websites, and professional organizations such as the American Society of Industrial Security (ASIS). States have databases available to the public that are extremely helpful; in Wisconsin, the Wisconsin Circuit Court Access page includes all records, both criminal and civil, for a person and is an excellent tool. Insider threat information will depend on any specific threats developed through time; many of the sources named will be utilized regarding insider threats, but only as persons develop intent. Also,

ITEBOOKS.DIRECTORY

as the insider normalizes, the individual will not be considered a threat, and the investigations should be closed.

The point of this chapter is to know when to compile existing intelligence program components into an overall assessment. Also, planning the overall assessment and documenting an annual intelligence program should be a repeatable process performed at least annually. The initial assessment will take some time, but after the processes are in place, the annual assessments should follow a clearly established format. The information may be different, but tracking the mission-critical components of your enterprise should be established.

ITEBOOKS.DIRECTORY

ITEBOOKS.DIRECTORY

16

Conduct an Intelligence Program Assessment

It is time to put the all the components and elements of the enterprise-wide assessment to paper in one central repository. By now, you have assessed the Security Department and ensured that your basic missions are defined and there are capable and willing personnel on your Security staff who have already engaged in the intelligence-based components closely tied to their primary missions.

Even if you have the luxury of hiring an analyst to steer your intelligence program, the value of engaging your asset protection security specialist in the tracking of external threats and criminal activity is crucial to the intelligence program. An analyst or third-party vendor can and will analyze and manage data and threats across all of your intelligence program components but will not be collecting the data and managing security programs on a daily basis. Therefore, the solid base of a security program rooted in intelligence-based mentality with security professionals educated in the intelligence-based methodology is crucial for success. Also, any analysis and recommendation of analysts will require an "action arm" to develop practical and cost-effective solutions for execution.

So, you have the security team squared away and the external threats subprogram is based within your asset protection team. As they are assessing and developing databases on criminal activity affecting your operations, they are collaborating with departments within your organization that have information on threats they have discovered through the course of their daily business activities.

ITEBOOKS.DIRECTORY

These "known" persons have been thoroughly investigated for capabilities and have demonstrated malevolent intent by their violent threats; warning flyers with their photographs and specific threatening behaviors have been distributed to company personnel who may have contact with these individuals. All capabilities possibly connected with general physical and cyberattacks relating to the external threats program, basically any way an outsider can attack your company, have been analyzed and documented. Specific threat capabilities from persons, groups, and organizations have been documented and put into a matrix for comparison in the vulnerability assessments. Evaluate and make determinations by analyzing all the external threat information; analyze all the threats, capabilities, and intent; and document the likelihood of attack from this sector and assess the risk.

Usually, the insider threats group will be represented by a person who is highly placed in security management in your organization. The tools of the disgruntled insider must be a component included in the enterprise-wide assessment. If there is no insider threat group at your company, you must document and measure the risk from insiders that exists in your enterprise. Is there any position within your enterprise that is so critical that the person in the position could devastate the company and cripple operations through malicious acts? If so, ensure information on this issue is documented and included in the final assessment. The criticality of the insider threat cannot be overemphasized; if your management does not engage, the recommendations should be brought up to the next level of supervision until you either receive results or run out of management who will listen to your presentation.

Risk is measured by the likelihood of attack plus the impact, so if the likelihood of attack is high but the impact low, as in previous examples of copper theft, risk can be measured as acceptable through the management of the security and intelligence programs put into place to handle the problem of copper theft. However, if the likelihood of attack is low and the impact is high, as in the incident of a mass shooting at your company headquarters, the planning and execution phases must include company-wide initiatives to properly prepare for such an incident. The risk in this area may depend on the amount of persons examined and tracked by the external threats group and the severity of the threats.

The more threatening an identified person or group becomes and the clearer their capability is uncovered, recommendations may include hiring armed guards, hardening your facilities with enhanced physical security devices, access that is more restricted to facilities and parking

ITEBOOKS.DIRECTORY

areas, initiation of executive protection, and further education of the general company population to active shooter scenarios.

Each of the components of the overall assessment must be measured for risk, and recommendations must be made for each component for management to be fully aware of probability of attack, the capability of the adversaries your company faces, and recommendations to reduce risk.

Unless you have assessed several companies in the past or developed a standard operating procedure for conducting an overall assessment, you will find the assessments and intelligence program takes on a life of its own and is unique to each enterprise. Due to rising and falling priorities, if two companies of similar size, facilities, and personnel started assessments at the same time, the first thing they would look at and assess would be their greatest threat at the time the assessment began. It is entirely feasible that the initiation of an intelligence or even a security program is due to a major catastrophe, such as an active shooter or other event of workplace violence, at one company would obviously spur an intelligence program with heavy emphasis on the insider threat program. However, the other company may have headquarters in a high-crime area, and the external threat program may be the initial emphasis due to employees falling victim to robberies, burglaries, and assaults. The point is that by the time you get to the point you are ready to conduct your enterprise-wide assessment, your initiation of an intelligence program, stabilization of your security program, and (depending on the strength of your subprogram leads) insider threats, external threats, and vulnerability assessment leads, you will have varying levels of proficiencies. All these need to be measured for improvement. Also, there is flexibility in the road map for the overall assessment.

Although there will be varying levels of proficiency, the components to include in the enterprise-wide assessment include the components discussed throughout this document: insider threats and external threats that deal with people. There will be general commonality in the way people attack your company. The capabilities of people will have crossover through these threat streams. The intent or motivation is the difference between the insider and the external threats; also, there is great value in knowing the specific capabilities related to both the external and insider threats. Mitigation steps are different for the external threats and insider threats. The external threats can be neutralized through good intelligence efforts and intervention by law enforcement, future tracking, and vigilance for future contacts. Insider threat mitigation is always geared toward stabilizing people as valuable assets to the company and

ITEBOOKS.DIRECTORY

the objective of bringing the insider back to work as a productive and content person.

The compilation of the components of your intelligence program is the enterprise-wide assessment. The recommendations made for each of the components (external, insider, and vulnerability assessments) must be compiled into a retrievable format, such as an Excel spreadsheet, analyzed and vetted for any redundant recommendations, consolidated, and prioritized. A change in access policy that addresses both the external and insider threats and adds an extra measure of protection to critical assets (vulnerability) that does not cost anything should be implemented and documented as soon as resources allow. Show your management that you are making or have made improvements that are cost effective but risk reducing because there will be items that are going to cost some money or force a change in culture.

However, do not be hesitant to make recommendations that cost money; it is your job to make reasonable cost-effective improvements and document the risk reduction as a result of the measures you recommend. If possible, develop options that are reasonable and allow the managers to make key but informed decisions regarding the company. Be reasonable and wise in your presentation; you should know what is acceptable to your management and what would not be acceptable.

The following is an example of the annual assessment from 2013 for my former company:

Example of the Enterprise-Wide Assessment

CORPORATE SECURITY: 2013 ASSESSMENT

This document is an assessment of the mission, capabilities, personnel duties, and responsibilities of the Corporate Security Office.

This document is intended to be an analysis and summary of Corporate Security.

This assessment is updated annually or as needed.

SUMMARY

The 2011 assessment determined the Corporate Security Office lacked several key components to an effective unit; there was a lack of a sense of mission, focus, organization, clear direction, leadership, structure, and discipline. There was also a lack of a central repository of written standard operating procedures and processes to accomplish the most basic duties within the department.

ITEBOOKS.DIRECTORY

During 2012, the lack of a central repository was addressed with the compilation of a Corporate Security Manual of Operations, which documented an organized Corporate Security process in one manual for reference of all personnel.

To address the issues in the lack of a sense of mission, focus, organization, clear direction, leadership, structure, and discipline, Corporate Security established and focused on the three core missions: asset protection, compliance/training, and physical access control. A shift in personnel in 2012, with the removal of two employees and addition of four employees, has improved the capabilities of Corporate Security.

Although the mission focus remained the same into 2013, the examination and analysis of internal and external threats to assets was initiated under the asset protection mission. Based upon the analysis and implementation of the internal and external threats working groups, along with several other intelligence-based working groups, mission focus in 2014 may evolve into inclusion of evolution of an intelligence mission.

CORPORATE SECURITY CORE MISSIONS

Physical Access Control: Corporate Security is responsible for monitoring and controlling physical access to company facilities and assets. The company has five business offices and a headquarters. Two of the offices have physical security perimeters (PSPs), which are protected with cameras, alarms, and badge card readers. The company has security responsibility for approximately 200 substations.

Asset Protection: In addition to the facilities mentioned, the company has 9,440 miles of transmission lines throughout the states of Wisconsin and Illinois and in Upper Michigan. The company has several ongoing transmission line and future transmission line construction projects. Corporate Security is responsible for the detection and prevention of thefts from assets across the corporate footprint.

Compliance: Corporate Security has roles in North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) compliance, specifically CIP-004 and CIP-006. Corporate Security is responsible for CIP-004, which outlines compliance in standards dealing with the R1 Security Awareness Program; R2 Security Awareness training conducted quarterly; R3 Personnel Risk Assessments (background checks); and R4 Physical Access/Revocation procedures. Corporate Security is responsible

ITEBOOKS.DIRECTORY

for CIP-006, which outlines compliance in standards dealing with the R1 Physical Security Plan; R2 Protection of Physical Access Control Systems; R3 Protection of Electronic Access Control Systems; R4 Physical Access Controls; R5 Monitoring Physical Access; R6 Logging Physical Access; R7 Access Log Retention; and R8 Maintenance and Testing.

Subsecurity Missions

Corporate Security also covers several submissions within the three primary core missions, specifically asset protection, physical access control, and compliance. These submissions are incident management and response, intellectual property and sensitive information protection, and executive protection.

2013 CORPORATE SECURITY PERSONNEL

The current staffing level of the Corporate Security Office is seven individuals, broken down by position as follows:

Corporate Security team leader
Security specialist, compliance
Security specialist, asset protection
Security specialist, physical access control
Security technical specialist
Security coordinator
Security coordinator

Team Leader

In June 2013, the CIP Program Office (CPO) was dissolved, and the Corporate Security Team began reporting directly to the director of System Operations. The Corporate Security team leader provides daily supervision to the Corporate Security team.

Security Specialists

There are three security specialists in the Corporate Security office. The security specialist position is the mainstay position in the Corporate Security office. The security specialists are responsible for the core security missions, physical access control, compliance, and asset protection. They provide the knowledge for day-to-day operations for the company regarding all aspects of physical security operations, including liaison with other departments, other utility companies, outside governmental compliance agencies, and law enforcement agencies. They are responsible for the execution of

ITEBOOKS.DIRECTORY

developed Corporate Security standard operating procedures, policies, processes, and guidelines.

Security Technical Specialist

This position provides the technical installation and maintenance of alarm equipment either through personal expertise or through the deployment of contractors.

Security Coordinator

These positions are support roles; they handle the responsibilities for clearances and badges for new employees/nonemployees and contractors and the daily operations of the Security Office.

CORPORATE SECURITY ACCOMPLISHMENTS IN 2013

Throughout 2013, the Corporate Security Department has strived to establish a sense of mission, focus, organization, vision, leadership, structure, and discipline. The following bullet points emphasize what Corporate Security has done to improve the functions in 2013:

Developed an Intelligence-Based Security Posture

In 2013, Corporate Security (CS) conducted and documented assessments evaluating threats and vulnerabilities to determine risk to the company. CS also developed plans and devoted resources to mitigate the identified risks in collaborative efforts across the enterprise, including but not limited to nonemployee management, corporate NERC CIP training, the Midwest Reliability Organization CIP audit, internal threats, external threats, and substation hardening, substation break-ins, Phase II Security upgrades, and a blended security approach across the company.

Assessed the Physical Security Department/Program

CS conducted a 2013 assessment of the company's physical security program, to be updated on an annual basis and mitigated to evolving threat streams and mission priorities. CS assessed the capability of personnel to accomplish new missions. In 2014, CS will strive to further develop and document the physical security program, with the task to analyze/advise and recommend physical security measures to departments/personnel in a collaborative manner.

Some of the important initiatives in the physical security program are as follows:

ITEBOOKS.DIRECTORY

Insider Threats

In 2013, CS conducted a collaborative assessment and led the effort that initiated an insider threat program working group with members from Physical Security, Information Security, Cyber Security, Human Resources, and Legal. The team developed a capability matrix of personnel and convened the working group on a monthly basis and when a person appeared to develop intent assessed the situation and developed/implemented controls to monitor the threat until stabilized.

External Threats

Throughout 2013, CS conducted assessments of who would do the company harm; the collaborative effort pulled from available data and compiled relevant threat information into usable reports/spreadsheets. CS utilized the gathered intelligence to mitigate/reduce threats through collaborative programs with law enforcement and other key departments. CS compiled threat assessments specific to each person and communicated these reports throughout the company, including mapping the information on a GIS [geographic information system].

Substation Break-Ins/Copper Theft Program

Carrying over strategies from 2012, CS conducted an assessment of the company's copper theft issues; utilizing data that included maps and theft information for past years, CS documented and tracked key elements, including but not limited to known copper thieves, nefarious scrap dealers, and law enforcement detectives. CS utilized the gathered intelligence to mitigate/reduce thefts through collaborative programs with law enforcement and other key departments.

Substation Hardening Initiative

In 2013, CS worked with Asset Management and initiated the Physical Security Assessment Working Group (PSAWG). The PSAWG was formed to assess and cost all mitigations to physical security vulnerabilities from a coordinated attack of an entire substation, including the substation perimeter, high voltage transformers, and the control house. Based upon specific risk assessments, the PSAWG emphasizes multiple industry best practice mitigation recommendations that can be utilized. Many of these practices include resiliency practices and a "blended" approach between physical and cyber security. CS is in a secondary role (Physical Security program management) regarding the PSAWG, assessing risks and making recommendations. Asset Management has the lead regarding the PSAWG, informing executive

ITEBOOKS.DIRECTORY

management of final recommendations and costs and then implementing additional physical security measures.

Physical and Cyber Security

Throughout 2013, CS and Cyber Security coordinated security efforts between company departments dealing in the physical and cyber arenas. The goal is to assess and defend against the cyber-led attack that defeats physical security measures or the physical-led attack designed to gain access to cyber assets. CS and Cyber Security have agreed to evaluate the possibility of developing collaborative assessment tools and in the future developing collaborative incident response plans.

2014 AREAS FOR IMPROVEMENT

The following areas have been identified throughout 2013. The evaluation process should continue, and adaptation of new initiatives should continue to allow the Corporate Security office to evolve with the security needs of the company as the company continues to expand.

General Improvement

- Implement incident response/crisis management plans: The Transmission Energy Response Plan and Business Continuity Management exercises have demonstrated a need at the company to develop a group to handle extreme incidents (bombings, shootings, weather-related disasters) and stabilize staff and resources, working to normalize operations, by managing the incident to allow TERP and BCM to accomplish their missions.
- Executive protection: An assessment needs to be conducted as it relates to internal/external threats to executive management and an evaluation of measures that may be taken to minimize risk.

2014 Corporate Security

Team Leader Goals

Formalize the PSAWG regarding the substation hardening initiative (asset protection).

Through the supervision of Corporate Security personnel and in conjunction with members of Asset Management, develop, initiate, document, and implement a working group to properly implement substation physical security enhancements.

ITEBOOKS.DIRECTORY

1. This goal will improve the company's ability to develop resilient physical security measures in substations to ensure speedy recovery from potentially damaging human-initiated events.
2. Collaboration on this goal includes select participants of Corporate Security staff and Asset Management.
3. Overall success will be measured by the formalization of the PSAWG and the documentation of the groups' mission/actions by the end of 2014.

2014 Copper Theft Initiative

Through the supervision of Corporate Security personnel, I will maintain the reduction of break-ins at owned substations at or below the average of the last three years (the average being 16). I will enhance the Corporate Security substation break-in program through the supervision of Corporate Security personnel, who will conduct scientific analysis of the facts of the thefts gathered through copper theft/break-in investigations, along with the use of GIS mapping, to develop patterns of criminal activity.

1. This goal will improve department efficiency and allow Corporate Security to strategically plan and implement pro-active measures to combat copper thefts/substation break-ins.
2. Collaboration on this goal includes select participants from the Corporate Security staff, other Wisconsin Utility Company security personnel, and members of law enforcement.
3. Overall success will be measured by maintaining the reduction of break-ins at owned company substations at or below the average of the last three years (the average being 16).

Develop a Critical Cyber Access Database

We will develop a critical cyber access database to replace manual spreadsheets as the Critical Access List. Through the supervision of Corporate Security personnel, we will develop and initiate progress improvement processes to automate the current access clearance list by developing an appropriate database.

1. This goal will improve department efficiency and allow Corporate Security to become more effective and accurate on processing access requests to the appropriate clearance levels.
2. Collaboration on this goal includes participants from the Corporate Security staff and engagement across company

ITEBOOKS.DIRECTORY

departments requesting access/clearance for employees and nonemployees.
3. Overall success will be measured by the development and implementation of an automated process to grant clearance and track access by the end of 2014.

Initiate an Electrical Utility Industry Former FBI Agent Security Working Group

Nationally, many directors/managers of security are former FBI agents with a strong fidelity to each other. Through individual effort, initiate and lead a network/forum of former FBI personnel employed in security in the electric/gas utility industry.

1. This goal will improve department efficiency and allow Corporate Security to share ideas and best practices throughout the electrical utility industry.
2. Collaboration on this goal includes the Corporate Security team leader and the heads of security of many large electrical utility industry companies.
3. Overall success will be measured by the development and implementation of this forum by the end of 2014.

The documentation and management of all the components into a malleable tool will allow you to track effectiveness of each of your threat components (external, insider, vulnerabilities, and risk assessments) as they evolve and allow the process of an annual assessment to be repeatable. I remember a saying of my track coach in high school that is applicable here: "It's a lot easier to stay up than to catch up."

ITEBOOKS.DIRECTORY

ITEBOOKS.DIRECTORY

Section VI

Enterprise Mitigation and Risk

ITEBOOKS.DIRECTORY

ITEBOOKS.DIRECTORY

17

Minimize Risk

With a capable security department in place and a comprehensive threat and vulnerability assessment completed, the final component of an intelligence-based security posture is to reduce risk through cost-effective measures. Now, the object is to mitigate threats and vulnerabilities identified in the risk assessment. Through the early engagement of your organization's management, it is hoped that they have been informed of risks identified through the assessment process and will be supportive of any costs that may be necessary to reduce risk to your organization.

One of the final products of the risk assessment is to develop programs to minimize risk to your company and assets. Evaluating threats, capabilities, and risk, along with determining likely methods of attack, does not serve the objective of reducing risk if your company is unwilling to address incidents that will occur within your company's footprint. If the building is burning around you and your threat assessment had outlined a likely attack from an external threat involving an arsonist, you have to have developed measures to reduce the risk of the identified threat. If not, a curt "I told you so" is the only satisfaction that you will have as your company's assets burn.

Identifying the capabilities of your adversaries, developing cost-effective countermeasures, and having a response plan that ensures resiliency and business continuity should be the goal of any risk-based methodology assessment. However, eventually something of a catastrophic magnitude will happen to your company, whether driven by humans or driven by nature (e.g., an active shooter or a tornado); the ability to respond to the crisis and how quickly you can resume productive operations will determine the success of your programs.

ITEBOOKS.DIRECTORY

The assessments of vulnerabilities and measures to reduce the risk of total disruption of critical equipment and assets should take the human-made and natural threats into account. Putting 12-foot concrete walls around a critical asset to reduce the threat of a person shooting your assets is a great idea unless the walls have not been measured against a tornado; an F2 tornado could turn the concrete walls into concrete projectiles that tear through your critical assets.

The objectives of reducing risk cannot be one dimensional; the specific threat assessments for internal and external threats concentrate on people and their capabilities. These capabilities include, but are not limited to, cyberattacks, sabotage, bombings, shootings, physical assault on employees and their families, financial crimes, economic espionage, theft of trade secrets, intentional damage to reputation, frivolous lawsuits, and harassment. Risk reduction by measuring vulnerability assessments must also include natural disasters. Ensure that any physical measures that are deployed are able to withstand nature in the area.

Some of the elements that should be considered are the establishment, training, and exercising of a crisis management team capable of handling any incident across the threat spectrum and offering the company a repeatable process to handle emergencies effectively. A well-maintained and experienced crisis management team is essential to any security or intelligence program. An excellent strategic plan is quickly negated if personnel are not capable of executing it in a timely matter in a crisis.

Along with a crisis management team, engage the business continuity team and any incident response group that you may have on site. A coordinated and unified command structure has to be planned and practiced prior to experiencing a significant event.

Incidents that are not handled properly can quickly grow into a swirling, snarling, out-of-control monster. An effective coordinated incident response between groups responsible for handling an emergency situation must also include the primary operations personnel responsible for daily operations as they will be working hard to fix or replace the damaged equipment. Where will they store valuable replacement parts? Will they need security guards for an extended period of time? Will there be other security needs in a crisis? Prior planning can eliminate time wasted in an incident.

Also, as indicated in the steps of the assessment process, you will find areas that need improvement; as at my former company, you will make immediate changes or additions to your security program. Other measures that are cost effective include an evaluation of standard security

ITEBOOKS.DIRECTORY

practices and any risk that may be reduced by evolving policies and procedures regarding these practices. When appropriate and the situation calls for it, minimize risk by identifying, tracking, and reporting threats to appropriate law enforcement and intelligence agencies.

However, there will be security measures that will cost money; these will be specific to your organization's needs. It is recommended that security packages that mitigate risk to several levels and options be designed for management approval; these measures should be realistic and can delineate risk reduced through the installation of additional security measures.

Change in any organization is never easy; ensure that you evaluate the consequences of enhanced security. Ask yourself these questions: How will enhanced security affect the daily operations of the organization? Weigh any changes affecting daily operations—are they necessary? Will there be "pushback" by other departments in the organization? Is a training module necessary or appropriate? Is a communications plan necessary or appropriate? Answering some of these questions prior to implementing changes in your organization may assist in the implementation process.

ITEBOOKS.DIRECTORY

ITEBOOKS.DIRECTORY

18

Develop a Strategic Plan

Throughout the process, it is important to have an end in sight. Although intelligence is constantly evolving, you have to ensure that you set some strategic goals or you will never stabilize your intelligence operations. To develop an intelligence program you have to have a vision that you can articulate to your executives, departmental heads, industry partners, and most importantly your staff, who will be implementing the intelligence program. The strategic plan is the "vision" that you outline and share with others; you can develop high-level bullets, for example, "Initiate and develop a collaborative insider threat group to address internal threats." Details are best left for any tactical plans cascading off each strategic component.

There is a level of risk in taking on the initiation of too many intelligence missions at one time. Unless you had a significant breach by an insider or an attack by an external threat and the company is throwing money and resources at you, there will be a limit to what you can do and how you can accomplish your core security missions while addressing intelligence missions. Through initial assessments, there must be prioritization of threats and when to address them in a staggered approach.

An ideal intelligence program addresses internal and external threats and vulnerabilities and does so through a blended collaborative approach regarding your intelligence program. The vision to complete initiation of a robust intelligence program should be outlined in your strategic plan.

Examining threats specific to your company and positively addressing issues that have existed in the past with no resolution is the best way to be noticed and garner support. If you address a theft ring and can show a reduction in the number of thefts on an annual or even monthly basis, ask your financial department to calculate the amount of money lost in

ITEBOOKS.DIRECTORY

each theft, not only through material but also any costs associated with the theft, including security personnel's investigative time, maintenance time to repair broken items or damaged material, replacement costs, and so on. After you have the total amount, multiply the number by the thefts that you prevented from the previous year and share the data with executives. People may say that the Security Department only spends money; the amount of resources that can be saved for the company through a solid security and intelligence program that prevents acts of violence, workplace violence, theft, or sabotage is measurable and should be included in your strategic plan, your vision, and daily operations.

The following examples are from the three years I was at the utility company; you can see the progression over time of the security missions with the integration of the intelligence-based missions:

Corporate Security Three-Year Strategic Plans, 2012–2014

2012

- Establish corporate security mission focus.
- Reorganize Corporate Security in alignment with missions.
- Acquire appropriate Corporate Security staff.
- Standardize Corporate Security operations.

2013

- Begin to document a Corporate Security risk assessment of all company assets.
- Establish and maintain Corporate Security working contacts with other departments.
- Standardize a training program for Corporate Security staff members.
- Establish an internal intelligence working group with members from Corporate Security, Information Technology, Human Resources, and Facilities.
- Standardize asset protection methods for assets with appropriate departments.

2014

- Establish and maintain Corporate Security working contacts with other electric utilities and local distribution companies (LDCs).
- Standardize training for personnel outside Corporate Security.

ITEBOOKS.DIRECTORY

- Expand the Intelligence Working Group to external contacts.
- Complete and document a Corporate Security risk assessment of all assets by the end of the year.

STEPS TO MEET STRATEGIC GOALS

- Assessed Corporate Security past, present, and future.
- Through the data gathered in the assessment, documented the delineation of Corporate Security missions: asset protection, compliance, and physical access control.
- Team leader reorganized Corporate Security Department in alignment with the CORE missions.

Past Positions	Reorganization Positions
Security manager	Team leader
Security coordinator	Security coordinator, monitoring
Security coordinator	Security coordinator, access
Security specialist	Security specialist, asset protection
Security specialist	Security specialist, compliance
Security specialist	Security specialist, physical access control
Security technical specialist	Security technical specialist (remains the same)

- Set challenging 2012 departmental Rewarding Excellence Achievement Collaboration Hard work goals.
- Rewrote job descriptions to align with the CORE Corporate Security missions.
- Established a central depository for all written documentation.
- Set standard operating procedures for Corporate Security and held personnel to established standards.
- Ensured the right personnel were in the right positions with the right attitudes.
- Ensured Corporate Security personnel know their duties and how to accomplish them.

ITEBOOKS.DIRECTORY

Corporate Security Three-Year Strategic Plan, 2013–2015

2013

- Begin to document a Corporate Security risk assessment of all assets.
- Establish and maintain Corporate Security working contacts with other departments.
- Standardize a training program for Corporate Security staff members.
- Establish an internal intelligence working group with members from Corporate Security, Information Technology, Human Resources, and Facilities.
- Standardize asset protection methods for assets with appropriate departments.
- Conduct a physical access control assessment and utilize the assessment to streamline and improve access/badging processes by the end of the year.
- Conduct a pilot program to evaluate background/drug screen vendors.
- Conduct a compliance assessment to define the Corporate Security compliance mission by midyear.
- Conduct a Corporate Security training assessment to define training needs and requirements and develop an annual training plan.
- Conduct an external threat assessment to determine risk associated with the company relating to external threats by the end of the second quarter.
- Begin planning a 24/7 monitoring command post in the Corporate Security suite.

2014

- Establish and maintain Corporate Security working contacts with other electric utilities and LDCs.
- Standardize training for personnel outside Corporate Security.
- Expand the Intelligence Working Group to external threats.
- Complete and document a Corporate Security risk assessment of all assets by the end of the year.
- Implement a pilot program to test the 24/7 monitoring command post in the Corporate Security suite.
- Complete the Corporate Security portion of the Phase II project.

ITEBOOKS.DIRECTORY

2015

- Fully implement the 24/7 monitoring command post in the Corporate Security suite.
- Expand, engage, and leverage external contacts to improve Corporate Security operations.

Corporate Security Three-Year Strategic Plan, 2014–2016

2014

- Conduct a compliance assessment to define the Corporate Security compliance mission by midyear.
- Work collaboratively with Human Resources to conduct a Corporate Security training assessment to define sponsor training needs specific to Corporate Security missions and develop an annual training plan.
- Begin planning a 24/7 monitoring command post in the Corporate Security suite.
- Complete the Corporate Security portion of the Phase II project.
- Establish and maintain Corporate Security working contacts with other electric utilities and LDCs.
- Evaluate the expansion of the Corporate Security missions to include an intelligence mission to work cross functionally across existing Corporate Security missions, to include but not limited to external threats, internal threats, criminal activity, and blended Physical Cyber Security assessments.
- Reduce/rewrite the three security trainings. Combine the appropriate aspects of the three trainings, ensuring the end product covers NERC CIP [North American Electrical Reliability Commission Critical Infrastructure Protection] requirements and good security practices.
- Transition security awareness training roll-out to Human Resources.
- Transition nonemployee on-/off-boarding to Human Resources.
- Formalize the Physical Security Assessment Working Group (PSAWG) with Asset Management to establish the physical security hardening initiative.
- Establish a CIP database to replace the Critical Cyber Asset Access list kept on Excel spreadsheets.
- Conduct a CCURE upgrade due in 2014.

ITEBOOKS.DIRECTORY

- Continue to evaluate the ramifications of NERC CIP V5 on security responsibilities.
- Evaluate the need to implement a crisis management program at the company.
- Begin the Physical Security engagement into the Cottage Grove (office) building expansion project.
- Begin the reorganization of the Corporate Security Manual of Operations (MoO).
- Continue to develop/assess a "blended" security approach with Cyber Security.
- Begin the transition of NERC CIP training content to Critical Infrastructure Compliance Program.

2015

- Continue the Physical Security engagement into the CG building expansion project.
- Continue to evaluate the ramifications of NERC CIP V5 on security responsibilities.
- Complete the reorganization of the Corporate Security MoO.
- Complete the transition of nonemployee on-/off-boarding to Human Resources.
- Continue the PSAWG with Asset Management to execute on the physical security hardening initiative.
- Evaluate/implement an investigations capability for internal and external investigations; make available to all appropriate departments.
- Evaluate/implement an executive protection subprogram at the company.
- Implement a blended security approach with Cyber Security.
- Complete the transition of nonemployee on-/off-boarding to Human Resources.
- Establish an intelligence mission in Corporate Security; appropriately train personnel.
- Implement a pilot program to test the 24/7 monitoring command post in the Corporate Security suite.
- Working with CCP, evaluate the CIP Protected Information (CPI) program for transition out of Corporate Security.
- Transition NERC CIP Training content to the CCP.
- Continue to evaluate the ramifications of NERC CIP V5 on security responsibilities.

ITEBOOKS.DIRECTORY

2016

- Continue the Physical Security engagement into the CG building expansion project.
- Fully implement the 24/7 monitoring command post in the Corporate Security suite.
- Fully implement and evaluate the intelligence mission to work cross functionally across existing Corporate Security missions.
- Finalize the establishment of a Corporate Security investigative submission across all departments.
- Continue the PSAWG with Asset Management to execute on the physical security hardening initiative.
- Expand the blended security approach with Cyber Security.
- Implement the requirements of NERC CIP V5 on security responsibilities.
- Expand, engage, and leverage external contacts to improve Corporate Security operations.

In addition to vision, the strategic plan must truly address the primary security missions through the development of the intelligence-based program. As mentioned several times, intelligence developed must be acted on in a timely manner to be effective. The prevention of adversary attacks is the objective. Intelligence itself is not the answer. It is developing the ability to effectively act upon the identified threat stream and reduce risk. The objective is not to become an intelligence guru know-it-all who looks down on the uninformed; it is to identify threats, capabilities, and intent of those who would do you and your company harm and either stop them or minimize the effectiveness of their attacks to ensure continued operations.

ITEBOOKS.DIRECTORY

ITEBOOKS.DIRECTORY

19

Develop a Tactical Plan

Having a vision that is clearly mapped in a strategic plan is critical to the establishment of a robust intelligence program. With that said, one of the most crucial elements to a successful intelligence, security, or any department/program is having the right people in the right positions with the right attitudes and the willingness and capability to adopt your vision and execute your strategic plan. Execution is key to any plan, and the methodology I used at the utility company was to develop an "action plan" template based on the five-item military operations order:

1. Situation: What is going on?
2. Mission: What are we going to do about it?
3. Execution: Make specific assignments to specific persons on actions that will be taken to accomplish the mission.
4. Administrative: What resources will be needed to accomplish the mission?
5. Command and control: How will the operation be controlled?

After the action plan template was created, I wrote several action plans, and we executed the missions as a team. I then required the team members to write action plans for their areas of responsibilities where there was a significant initiative. The following are examples of action plans from three company initiatives: the copper theft program, the compilation of the Manual of Operations, and shootings on transmission lines:

ITEBOOKS.DIRECTORY

2012 Copper Theft/Break-In

ACTION PLAN

Situation: A recent assessment by Corporate Security has identified a need for a copper theft/break-in analysis and mitigation plan to define Corporate Security strategies and actions.

Mission: In a collaborative effort, the Corporate Security team will create a repository of strategic measures to be considered, prioritized, and implemented in an effort to reduce copper theft and break-ins, therefore enhancing the company's asset protection plan. This advances the organization by applying strategic planning to the deployment of Corporate Security's limited resources.

Execution: Under the supervision of the Corporate Security team leader and in collaboration with Corporate Security staff members, the project lead security specialist will lead the mission to gather intelligence, analyze data regarding copper thefts and break-ins, discuss strategic measures, and prioritize those measures in implementing an action plan to serve as a road map of direction toward the reduction of incidents. The team leader, the lead security specialist, and others from Corporate Security or other invited departments have initiated monthly meetings and have begun to assess and brainstorm potential solutions for implementation.

It is anticipated monthly meetings will begin in the first quarter of 2012 and continue throughout the remainder of 2012. These monthly meetings will be the setting for a partnership of Corporate Security and other resources; collection of data or statistics will be continually updated, analyzed, and prioritized. The initial analysis will include the identification of company field assets and mapping incident locations from 2010 and 2011. Going forward, information that will be collected and plotted will be (1) Incident coordinates (longitude/latitude); (2) salvage yard locations; and (3) Phase II Substations with Enhanced Security sites. Throughout this project, other categories may be identified and added to the plotting and analysis. Further examination will be conducted concentrating on identification of any patterns of criminal activity. This will improve department efficiency and allow Corporate Security to strategically plan proactive measures to combat future copper thefts/break-ins. The initial analysis is anticipated to be accomplished by the end of the first quarter 2012, with preliminary steps of action(s) identified and implemented.

This process will continue throughout 2012. Each month, the project lead security specialist will summarize and forward to the team leader information on the incidents that have happened and what

ITEBOOKS.DIRECTORY

has been discussed and prioritized at the monthly meetings and the implementations acted upon. Progress and success will be measured in two categories: (1) the number of strategic measures developed and (2) the number of strategic measures implemented by the end of 2012.

It is expected the entire staff of Corporate Security will be involved to varying degrees in this process. As gaps are identified, the team leader and the project lead security specialist will evaluate the measures identified and prioritized in association with combating incidents and frequency. Assignments will be made based upon expertise and departmental needs. Coordination of assignments to other departments will also be recorded and tracked. This tracking will be maintained by the project lead security specialist. The following Corporate Security personnel will be assigned responsibilities and tasks throughout 2012:

1. Team leader
2. Asset protection security specialist, project lead
3. Compliance security specialist
4. Physical access control security specialist
5. Security technical specialist
6. Security coordinator

Command and control: The Corporate Security team leader and project lead security specialist will meet weekly, with additional Security staff invited as deemed necessary. At each 2012 monthly meeting, team members will discuss incidents, status, investigations, trends and patterns, strategic options, and assignments and track progress on assigned tasks. In addition, any communications made or joint efforts with other departments, Wisconsin Utility Company security personnel, and/or members of law enforcement will be discussed and shared. The team leader will periodically report progress to executive management through the proper chain of command.

Administrative: The team leader will assume overall responsibility for this project. Project lead will conduct the day-to-day operations regarding this project and will make assignments to other Corporate Security staff members in conjunction with team leader. Efforts will include collaboration with Geographic Information Systems, Maintenance, and Engineering, along with Wisconsin Utility Company security personnel and/or members of law enforcement. Progress will be tracked and measured by the number of strategic measures developed and by the number of strategic measures implemented on a monthly basis.

ITEBOOKS.DIRECTORY

2012 Manual of Operations

ACTION PLAN

Situation: A recent assessment of Corporate Security has identified a need for a central repository for paperwork defining Corporate Security standard operating procedures.

Mission: In a collaborative effort, the Corporate Security team will create a central repository for Corporate Security paperwork, including but not limited to standards, policies, procedures, processes, guidelines, and templates, which will serve as the standard operating procedures of Corporate Security.

Execution: Under the supervision of the Corporate Security team leader and in collaboration with Corporate Security staff members, the project lead security specialist will develop steps and implement this action plan for the creation of the Manual of Operations to serve as the central repository for Corporate Security paperwork. The team leader and security specialist have initiated weekly meetings and begun to assess and define the finite universe of Corporate Security paperwork.

It is anticipated by mid-March 2012 that the initial compilation of Corporate Security paperwork will be complete, allowing an in-depth factual analysis. The initial analysis will include classification of the compiled documents into three categories, the three core Corporate Security missions: (1) compliance, (2) physical access control, and (3) asset protection. Throughout this project, other categories may be identified and added to the Manual of Operations. Further analysis will be conducted, concentrating on identification of any gaps in the existing classified paperwork. For example, if a procedure details the parameters for badging nonemployees but there are not any processes written as to how to badge a new nonemployee, this gap would be documented and tracked. Any gaps identified will be addressed through collaborative efforts with any involved parties and the authoring of appropriate paperwork. Any paperwork generated to address the identified gaps would also be documented and tracked. The initial analysis is anticipated to be accomplished by the end of the first quarter 2012.

This process will continue throughout 2012. Each Corporate Security monthly staff meeting will include a segment devoted to the progress of the Manual of Operations, with the entire Corporate Security staff. Progress will be measured through the documentation

ITEBOOKS.DIRECTORY

of gaps identified and type/number of documents written to address each gap along with the name of the author of the documents.

It is expected the entire staff of Corporate Security will be involved to varying degrees in this process. As gaps are identified, the team leader and project lead security specialist will evaluate the tasks associated with addressing the gap and assign the writing of appropriate paperwork to the most qualified Corporate Security staff member. Assignments will be made based upon expertise and departmental needs. A reasonable deadline for completion will be assigned along with each task. Any gaps not easily assigned according to appropriate job function will be assigned through a rotating alphabetical roster, with final assignment approval by the team leader. This list will be maintained by the project lead security specialist. The following Corporate Security personnel will be assigned Manual of Operations responsibilities and tasks throughout 2012:

1. Team leader
2. Security specialist compliance, project lead
3. Security specialist, asset protection
4. Security specialist, physical access control
5. Security technical specialist
6. Security coordinator

Command and control: The Corporate Security team leader and project lead security specialist will meet weekly with additional Security staff invited as deemed necessary. At each 2012 monthly Corporate Security staff meeting, a segment will be dedicated to the Manual of Operations to discuss trends and assignments and track progress on assigned tasks. The team leader will periodically report progress to executive management through the proper chain of command.

Administrative: The team leader will assume overall responsibility for this project. The project lead will conduct the day-to-day operations regarding this project and will make assignments to other Corporate Security staff members in conjunction with the team leader. This effort will include collaboration with Facilities and Information Technology Departments.

Progress will be tracked by the creation of the manual, identification of gaps, and filling of those gaps with appropriate paperwork. Milestones will be set throughout the process, and deadlines for paperwork assignment completion will be established and monitored.

ITEBOOKS.DIRECTORY

2012 Upper Peninsula Transmission Line Vandalism Action Plan

Situation: There have been numerous acts of shooting vandalism on company transmission lines 446, 457, and 468 located in the Upper Peninsula of Michigan.

Mission: In a collaborative effort with Transmission Line Maintenance and Customer Relations, the Corporate Security team will develop and implement strategic proactive measures in an attempt to prevent acts of vandalism against transmission lines.

Execution: Corporate Security, in collaboration with Transmission Line Maintenance and Customer Relations, will consider the following and any viable options to address incidents of vandalism on transmission lines 446, 457, and 468 located in the Upper Peninsula of Michigan.

1. Complete a formal fact-based analysis of transmission line incidents in the area in the last 10 years. Include any similar incidents in a 100-mile radius. Compile any documentation regarding these incidents, including police reports, security incident reports, IXO* reports, newspaper/media reports, any and all other available documentation. What has been done in the past? Write a narrative of the problem. Develop an action plan with what must be done; define the mission. Include assignments for involved personnel. Document the actions taken for future use. (All departments)
2. Evaluate any prior, existing, or future public awareness campaign utilized to educate the public on the dangers associated with downed transmission lines. (Customer Relations)
3. Evaluate developing options with the landowner to restrict entry to the area. Also, explore the possibility of hiring a contractor to change the physical aspects of the area to make it less favorable to shooters. Add dirt berms to the side of the road, speed bumps throughout the area to restrict traffic, other methods to make the area less desirable for the activity currently seen. (Customer Relations)
4. Examine if there is a local "angry man/woman" with a vendetta against the company/industry who was committing these acts as a form of revenge. (Customer Relations)

* IXO was a company with an external cyber reporting system. It was used to generate and track reports.

ITEBOOKS.DIRECTORY

5. A current camera deployed in the area has produced high-quality photographs. Corporate Security will evaluate the cameras deployed and determine how to enhance the coverage of the area to deter/detect or identify the subjects of any vandalism to transmission lines in the area. (Corporate Security)
6. Corporate Security will continue to pursue the development of the enhancement of video alarm camera systems with the capability to capture unique cellular telephone data when triggered by an event. Captured cellular telephone information will be provided to law enforcement for evidentiary analysis and use. (Corporate Security)
7. Evaluate existing laws concerning the criminal activity. Research what tools (laws) are available to law enforcement to have at their disposal to address this issue. If appropriate laws do not exist, evaluate involving the company's Legal Department to work with local municipalities to pass local ordinances/laws to address the problem. (Corporate Security)
8. Analyze the data from the deployed camera and develop days and times of high-frequency activity in the area. If appropriate, request local law enforcement increase patrols in areas designated as vulnerable through the analysis. (All)
9. Evaluate the use of contract security companies for sporadic roving patrols during the weekends. (Corporate Security)
10. Evaluate and develop a "rewards" program specific to the area of concern. (Corporate Security)

Regarding action item 1, Corporate Security has conducted an initial analysis of documented incidents of vandalism from maintenance records provided by Transmission Line Maintenance. The following chart represents the results of the analysis:

Date	Location (T-Line)	Position	Damage
06/28/2006	4XX	36	Three conductors
11/21/2006	4XX	37	Eight conductors; wire
05/29/2007	4XX	38	One conductor
08/19/2008	4XX	35	Insulator
08/19/2008	4XX	37	Conductor

Continued

ITEBOOKS.DIRECTORY

Date	Location (T-Line)	Position	Damage
08/19/2008	4XX	37	Conductor
08/19/2008	4XX	42	Insulator
08/19/2008	4XX	44	Insulator
08/19/2008	4XX	46	Insulator
08/19/2008	4XX	35	Insulator
12/03/2009	4XX	35	Conductor
04/03/2012	4XX	36–37	Conductor; wire

Corporate Security, in collaboration with Transmission Line Maintenance and Customer Relations, will continue to gather information and author a final report that will include an analysis of available data. The final report will also include any measures implemented in an attempt to curb the criminal behavior.

Administrative: Corporate Security, Transmission Line Maintenance, and Customer Relations will meet as often as deemed necessary. It is anticipated Corporate Security and Transmission Line Maintenance will meet in the area on April 26–27, 2012, to complete a risk assessment/site survey.

Progress will be tracked by the creation of an action plan and the analysis of available data. Any proactive measures implemented through the collaborative effort of employees will be documented for future tracking. Milestones will be set throughout the process, and deadlines for tasks/assignments will be established and monitored.

As you can see from the examples, the action plans laid out specific assignments, meetings, and goals to specific departments and, if appropriate, individuals. It was an effective method to execute plans to meet mission objectives. The plans provided focus and a clear delineation of duties and assignments.

The action plans also served another significant purpose; once written, they became a two- or three-page briefing paper for executives, other company department personnel, electrical industry partners, and law enforcement. The action plans were the tools I effectively used to ensure execution of the tactical plans to meet the strategic vision.

ITEBOOKS.DIRECTORY

20

Communication

Communication is one of the critical keys to success in any program and will be part of every component of your security/intelligence programs. From the initial assessment of your security program to the final phases of the implementation of your tactical plans to reduce risk through the recommended mitigations, all affected parties should be informed and aware of the security and intelligence programs and their impact on their work operations. The executives of your company should be involved and engaged early on through concise presentations (e.g., PowerPoint) explaining the benefits of the programs through the prevention of incidents or the preparedness to react and minimize the negative impact on your company's operations. The drafted action plans can also play an important role in briefing executives.

At the utility company, I initiated a report that we sent twice a month with the facts of copper theft incidents to allow tracking an issue that was important to the company and to the executives of the company. It also allowed Corporate Security to remain in the notice of the executives with a successful program. As Corporate Security expanded initiatives, the bimonthly report expanded to include those initiatives. This allowed us to engage the executives and gave them facts they could use in meeting with other industry executives. The following is an example of the executive bimonthly report:

Action Regarding June Copper Thefts

On July 6, 2012, Corporate Security convened the sixth monthly meeting of the Copper Theft Working Group, which is held the first Friday

ITEBOOKS.DIRECTORY

of each month throughout 2012. The purpose of this meeting is to review the incidents from the prior month, analyze the data, and brainstorm initiatives to mitigate incidents in the foregoing months. The meeting was attended by the security team leader, the security technical specialist, and the security specialist at the Madison Office.

JUNE COPPER THEFT ANALYSIS

There were no break-ins at controlled substations in June 2012. To date, there have been a total of 10 controlled substation break-ins, with the majority (7) occurring in January 2012. However, in June 2012, there was one reported copper theft at a company asset. This incident occurred on the transmission line located in Mauston, Wisconsin.

CRIMINAL INTELLIGENCE INITIATIVE

The security specialist continues to identify names of subjects arrested for copper theft through open-source reporting and law enforcement contacts; in June 2012, there were three names added to the subject (known offender) list.

SUBSTATION STANDARDS

The team discussed the substation decision tree as developed by meeting with the Substation Standards group. It was decided to suggest the development of a "working group" of at least members of Corporate Security and the Substation Standards Group to conduct an initial assessment of substation construction to determine the items on the substation decision tree. Also, standards regarding three items should be developed no matter where the substation ends up in the decision tree. Whether the substation is standard or CIP [Critical Infrastructure Protection] compliant, it should have the same doors and crash bars and no holes with greater dimensions than 96 inches. These standard items should be designed and documented.

ASSESSMENTS AND STRATEGY

The team reviewed the most recent copy of the GIS [geographic information system] maps, which demonstrated substation properties and the locations of the 2012 year-to-date incidents. It was decided the video systems would remain deployed in their current locations during the month of July 2012. The deployment and status of the video systems is as follows:

1. Rangeline: fixed
2. Granville: fixed

ITEBOOKS.DIRECTORY

3. Femrite: mobile
4. Erdman: mobile
5. Mullet: mobile
6. Lone Rock: mobile
7. Atlantic Mine: mobile
8. South Fond du Lac: mobile
9. Black system: in for repairs
10. E system: with Marquette County Sheriff

Plans for August 2012 include

1. Repair the Black system.
2. Pick up the Blue and E systems from the Upper Peninsula.
3. Obtain the Granville system, upgrade, and deploy to Femrite as a fixed system.

These actions will make three mobile video systems for redeployment by the first week of August 2012: Black, E, and Femrite.

SUBSTATION ASSESSMENTS

At the August 2012 copper theft meeting, a new initiative will kick off, with Corporate Security personnel meeting in the morning to review the current measures; in the afternoon, they will conduct security risk assessments on up to three area substations and document the results in a spreadsheet. The objective is to determine and document the most vulnerable substations within the company's footprint. This effort will continue until all substations are assessed.

ACTION TASKS FOR FOLLOW-UP

1. The security specialist agreed to obtain a dozen 10- to 12-inch copper tail examples and have them painted purple. The plan is to visit scrapyards, explain their identification, and leave them with a sample. The security specialist has recently received examples of 4/0, 2/0, and No. 4 hard-drawn copper.
2. The team leader will follow up on the status of the approval for the five additional video systems.
3. The security technical specialist accepted the task of making the Femrite video kit permanent and coordinating station power.
4. The security technical specialist accepted the redeployment task of the two video systems per the group's discussion and prioritization.
5. The security technical specialist accepted the task of obtaining an estimate for a Logitech camera system.

ITEBOOKS.DIRECTORY

6. The security technical specialist will discuss the creation of a spreadsheet.
7. The team leader agreed to follow up with the state regulators concerning any known nefarious scrap dealers.
8. The team leader agreed to take the task of exploring an "externet" for housing break-in information to be used by the company and local distribution companies.

The business stakeholders, security/intelligence working group partners, subject matter experts, law enforcement liaison, intelligence liaison, industry partners, media contacts, and general employees will all require communications geared to their needs, level of involvement, and participation in the intelligence and security programs.

As an example, the following memorandum was drafted and sent to executives at the utility company after an agreement was met between me as the security lead and the Human Resources manager after it was decided that Human Resources should assume responsibility for background screenings, drug tests, and training for nonemployees, which Corporate Security had been handling—a classic example of "mission creep." The following memorandum is a good example of communication necessary to address specific departments or issues:

On October 22, 2013, the manager of Human Resources met with the Corporate Security team leader to discuss the initial transition of specific nonemployee access duties traditionally performed by Corporate Security to Human Resources. The meeting led to agreement on the following points:

1. All Personal Risk Assessments (PRAs) will be conducted by Human Resources, including those of nonemployees. Human Resources will conduct the PRAs and forward a completion form to Corporate Security to grant access, similar to the current process for employees.
2. All drug tests will be conducted by Human Resources, including those for nonemployees. Human Resources will notify Corporate Security as stated in point 1.
3. All security-related training will be assigned to employees and nonemployees by Human Resources. Corporate Security will be responsible for content and following guidelines set forth by Human Resources. Corporate Security must retain the ability to view completed training in Excelerate for compliance requirements.
4. Corporate Security will contribute a physical security access block of training for nonemployee company sponsors, contributing to the Human Resources future endeavors for compilation of a sponsor training program.

ITEBOOKS.DIRECTORY

Due to evolving environmental and resource allocation needs, an exact timeline of this transition is currently difficult to define; however, as assessment efforts stabilize, a timeline will be documented.

There will be instances when a communications plan should be initiated with the company's communications team, or through a third-party vendor, due to major changes in the security protocol based upon the recommendations implementation plan from the overall assessment. These must be professionally planned and executed to ensure the message is received and processed by the targeted audience.

DEVELOPMENT OF AN INTELLIGENCE-BASED SECURITY POSTURE

In 2013 and continuing into 2014, Corporate Security (CS) conducted and documented assessments evaluating threats and vulnerabilities to determine risk to the company. CS also developed plans and devoted resources to mitigate the identified risks in collaborative efforts across the company, including, but not limited to, internal threats, external threats, substation hardening, substation break-ins, physical security upgrades, and a blended security approach across the company.

ASSESSMENT OF THE PHYSICAL SECURITY DEPARTMENT/PROGRAM

Since 2011, CS has conducted an annual assessment of the company's physical security program, designed to mitigate any evolving threat streams and mission priorities. CS assessed the capability of personnel to accomplish their missions. Some of the most significant initiatives in the physical security program are as follows:

1. Substation Hardening Initiative
   The company has initiated the Physical Security Assessment Working Group (PSAWG). The PSAWG was formed to assess and develop costs for mitigations to physical security vulnerabilities from a coordinated attack of an entire substation, including the substation perimeter, transformers, and the control house. Based upon specific risk assessments, the PSAWG emphasizes multiple industry best practice mitigation recommendations that can be utilized; those techniques would include but would not be limited to concrete walls, resilient fencing, and high-definition cameras with analytical capability; rapid and effective response to alarms; motion detection activated audio and light alarms.

ITEBOOKS.DIRECTORY

2. Substation Break-Ins/Copper Theft Program
   Carrying over strategies from 2012, CS conducted an assessment of the company's copper theft issues. Utilizing data that included maps and theft information for past years, CS documented and tracked key elements, including, but not limited to, known copper thieves, nefarious scrap dealers, and law enforcement detectives. CS utilized the gathered intelligence to mitigate/reduce thefts through collaborative programs with law enforcement and other key departments.
3. Insider Threats
   In 2013, the company conducted a collaborative assessment and led the effort that initiated an insider threat program working group with members from Physical Security, Information Security, Cyber Security, Human Resources, and Legal.
4. External Threats
   Throughout 2013 and into 2014, the company conducted assessments of who would do the company harm. The collaborative effort pulled from available data and compiled relevant threat information into usable reports/spreadsheets. CS utilized the gathered intelligence to mitigate/reduce threats through collaborative programs with law enforcement and other key departments. CS compiled threat assessments specific to each person and communicated these reports throughout the company, including mapping the information on GIS.
5. Physical and Cybersecurity
   Throughout 2013, CS and Cyber Security coordinated security efforts between company departments dealing in the physical and cyber arenas. The goal was to assess and defend against the cyber-led attack that defeats physical security measures or the physical-led attack designed to gain access to cyberassets. CS and Cyber Security have agreed to evaluate developing collaborative assessment tools and in the future developing collaborative incident response plans.

The following is an outline prepared to show what we implemented and the status. It was prepared to be handed out, cut and pasted into an e-mail or Power Point, and/or read for an oral presentation:

Throughout 2012, the day-to-day operations of the Physical Security Department improved, and the continuous improvement continues in 2013. As daily operations stabilize, the Physical Security

ITEBOOKS.DIRECTORY

Department has expanded into areas not previously addressed. New Physical Security Department initiatives tied directly to this issue are:

1. Introduction of intelligence-based security initiatives.
2. Close coordination with Cyber Security.
3. Close coordination with Asset Maintenance and other departments regarding the shooting incidents in Marquette County, Michigan.
4. Coordination with Substation Standards to define universal door, crash bar, and entrance points and a physical security risk assessment on any new substation construction.
5. Physical security risk assessments for Phase II substations and new construction projects that include demographics and crime statistics and examine past criminal activity to measure vulnerabilities to physical attacks.
6. Initiation of the External Threats Working Group to consolidate information on threats from outside the company's enterprise.
7. Initiation of the Insider Threats Working Group to evaluate and mitigate threats that may affect/emanate from personnel and contractors.
8. Reduction of traditional copper thefts/substations breakins (29 in 2011 to 14 in 2012) through gathering of criminal intelligence and spreadsheets of the names of known copper thieves, of detectives specializing in copper theft, and of nefarious scrapyards. Close coordination occurs with Asset Maintenance and Construction regarding copper thefts.
9. Utilization of GIS data for threat and theft tracking.
10. Increased liaisons with other utility security and local law enforcement.
11. Constant evaluation, expansion, and deployment of the technical capabilities of security equipment, video systems, high-resolution cameras, and intrusion detection devices.

By ensuring clear, concise communications throughout the initiation and implementation of all of your security and intelligence programs, you will allow the seeds of your vision to take root and grow. Nothing can kill any program quicker than miscommunication, misunderstanding, and the hard feelings that these missteps can cause with the people you are trying to protect and the executives who will be critical in supporting your security and intelligence programs. The most effective strategic and tactical plans are the ones that are effectively communicated and put into place through effective execution. Finally, do not hesitate to ensure the executives or anyone interested in security or intelligence is aware of the success of these programs.

ITEBOOKS.DIRECTORY

ITEBOOKS.DIRECTORY

Section VII

Implementation: Case Studies

ITEBOOKS.DIRECTORY

ITEBOOKS.DIRECTORY

21

Utility Company Execution

Having the appropriate personnel on your staff is the most crucial element to success for any program that you are managing. A staff that can share your vision will understand your strategy and will assist with the strategic plan. Engagement in the strategic plan will ensure ownership of their subprogram. Whether you utilize the action plans to develop a template that is unique to your own company's mission is up to you. However, ensure that you do develop a standard. Engaging your staff is essential, but lay out the ground rules, set expectations, and standardize your plan and document to outcomes. Show the staff what success looks like so they send you what you are looking for at the end of the day. Otherwise, the type A personalities will quickly set up what their vision of their subprogram looks like to them, and if not standard to the team, they will be hurt and disengage if you "critique" them after the fact. Lay out the information ahead of time and ensure everyone puts their ideas, plans, and execution into a standard format. Standardization should not stifle their original ideas, but it will make it easy to track and allow you to maintain a semblance of order for the several subprograms that you have to manage to develop a robust intelligence program.

The key to execution is having the right staff in place who know what your expectations are along with a shared team vision. As stated previously, from the first month that I arrived at the utility company, I established a firm tone and ensured the staff knew where they stood with me. I set the expectations, reemphasized the missions and objectives, and told personnel I would hold them accountable. I held monthly staff meetings with a set agenda and recorded the results of the meetings, along with tasks and expectations. The following document represents the first staff

ITEBOOKS.DIRECTORY

meeting notes after I conducted the first staff meeting; I had been on the job for a month:

Subjects for November 17, 2011, Meeting

Any time a new boss comes into a department, whether it is the military, public, or private sector, it is important the new boss lay out their vision and set the parameters regarding what is expected by their staff. To ensure there are no misunderstandings, I wanted to ensure we all were clear on my positions and communicate the baseline of what I expect from Corporate Security personnel.

1. I am going to provide structure/focus to the department through the evaluation of our core missions, personnel assignments, and job responsibilities. I will be very involved in the day-to-day operations of the Corporate Security office until I feel comfortable with practices and procedures.
2. I would like everyone to utilize the chain of command. I am not saying you do not speak to anyone in the company, but if you are meeting with other managers or executives outside the company, make sure I am aware of the purpose of the meeting and who is in attendance. Do not set up meetings with management without letting me know first; I may have input and would like to discuss it prior to setting up meetings.
3. Do not take on any additional projects without discussing them with me prior to committing security resources. I want to be aware of any new projects we take on and track them.
4. Please make sure you tell me about the content of meetings that you wish me to attend prior to committing my attendance. Do not schedule meetings for me without asking me first.
5. I will be performing a 90-day assessment to be completed February 15, 2012, regarding the Corporate Security missions, duties, and responsibilities.
6. As time goes by, I will be evaluating each person in the Corporate Security office, including their roles, duties, and responsibilities along with their performance within their positions.

Each month for the time I was at this company, I had a monthly staff meeting. The agendas were:

ITEBOOKS.DIRECTORY

SUBJECT: October 2012 Team Meeting
ATTENDEES: Names of Attendees
MEETING HELD ON: October 15, 2012, 9:00 a.m. to 2:30 p.m.
LOCATION: Room 175
AGENDA

Item	Description
Opening remarks bimonthly meetings with Groups Asset Protection, Physical Access Control Compliance	Roundtable
Team discussion of job duties, roles, responsibilities	
Performance matters 1. Manual of Operations 2. Phase II 3. Substation break-ins 4. CIP [Critical Infrastructure Protection] transition to CPO [CIP Program Office]	2012 goals, status, and schedules
CCURE	Update and discussion
Open forum	Open for discussion

The following are the documented results of the meeting described in this agenda:

Content of October 15, 2012, Corporate Security Staff Meeting

The following items were discussed at the monthly Corporate Security staff meeting held on October 15, 2012; present at the meeting were [names of the attendees]. The first item of business was to go around the table and discuss what each team member was currently working on.

Team leader (TL) discussed the assessment of the formation of a Threat Intelligence Working Group with Corporate Security, Information Technology (IT), Human Resources (HR), and other appropriate departments to conduct corporate-wide vulnerability assessments with possible mitigations. TL Trier also discussed the Corporate Security-led project of evaluating the future necessity of a central monitoring station for CCURE alarms; this study will be compiled with input from Systems Operations personnel.

The security technical specialist discussed the CCURE 9000 upgrade with the group; the issues with the iStar panel switch over

ITEBOOKS.DIRECTORY

from CCURE 800 have been resolved, and the crossover will be initiated on October 16, 2012. The Phase II project requires writing risk assessments for the substation upgrades, and all Corporate Security personnel have been asked to assist in the Phase II assessment writing project. A meeting will be scheduled in the beginning of November 2012 to analyze and assign specific tasks.

The compliance security specialist continued to update the initial hard copy of the Manual of Operations (MoO); the MoO binders are in the Corporate Security suite for use by team members. The RSAW review was conducted, and Corporate Security had a few items to address, but the issues were minor. The compliance security specialist has been conducting new vendor training as there has been a surge in new vendors in the last couple of months.

The physical access control security specialist is leading an effort to conduct an audit of the supplier's general access list. The security coordinators are assisting with the supplier's audit. They are also working on a key audit. The physical access control security specialist continues to author and revise procedures, processes, guidelines, and checklists regarding the physical access control mission.

As of October 1, 2012, the security coordinators had switched shifts; however, in deference to their request, they will sit at the same desks during regular business hours (8:30 a.m. to 5:00 p.m.). By October 5, 2012, the security coordinators informed the TL they decided it would be best to switch desks when the monthly duties were transferred.

The security coordinators are working closely with the physical access control security specialist of other utility company to track their substation keys and keys in general.

The asset protection security specialist has been coordinating with other company departments, such as Customer Relations and GIS [global information services] mapping, in an attempt to consolidate threat information pertaining to company "open houses."

The TL then conducted a review of the goals for each individual team member, including a measurement with the team members to see how close they were to attaining their goals. The four goals reviewed were Phase II project, reduction of copper theft, creation of the MoO, and the evaluation of tasks eligible to transfer from Corporate Security to the CIP Program Office (CPO). There were some goals that needed attention, but guidance was given to each team member by the TL regarding how to accomplish their goals by the end of 2012.

The TL led a group discussion to explore 2013 Corporate Security goals; the results of the discussion are as follows:

ITEBOOKS.DIRECTORY

1. Initiate a Threat Intelligence Working Group with Corporate Security, IT, HR, and other appropriate departments to conduct corporate-wide vulnerability assessments with possible mitigations. (Responsible team members: [names])
2. Initiate, develop, and document a formal Corporate Security training program for positions within the department. (Responsible team members: [names])
3. Working with company HR, initiate, develop, and document Corporate Security training to on-board new employees. (Responsible team members: [names])
4. Initiate, develop, and document new access clearances for CCURE 9000. (Responsible team members: [names])
5. Improve and document the annual maintenance/testing process for critical Corporate Security technical assets. (Responsible team members: [names])
6. Initiate and document a life-cycle management program for critical Corporate Security technical assets. (Responsible team members: [names])
7. Initiate and document a security designs standard for Corporate Security projects. (Responsible team members: [names])
8. In conjunction with the CPO, participate in a CIP Version 5 gap analysis representing Physical Security. (Responsible team members: All)
9. Improve, improvise, and document Corporate Security incident reporting and intelligence tracking. (Responsible team members: All)
10. Initiate, define, document, and implement a standard key management program for company substation and facilities keys. (Responsible Team members: [names])

The meeting concluded after four hours; the next meeting will be mid-November 2012.

The keys to execution at the utility company were the standardization of the security program and the stabilization of the security staff. Engagement of the security staff and management regarding the importance of the security missions and implementation of the external threats program through the copper theft initiative and Marquette shooting incidents was critical to our programs. Since we developed programs that were successful in these areas when other incidents that greatly concerned the electrical industry (e.g., the Metcalf substation shooting in California and Jason Woodring in Arkansas) became national issues, we were able to

ITEBOOKS.DIRECTORY

quickly call a collaborative group together, assess the issue, and develop a factual intelligence-based plan of action to address any issues at our sites.

The process we developed was repeatable and allowed us to quickly adapt to changing and evolving threat streams. The methodology was to (1) identify the issue; (2) outline the mission/objectives; (3) gather data and intelligence; (4) analyze the data and compile a report; (5) make recommendations; and (6) implement and execute. It was a methodology that we applied to everything that was worthy of analysis; it was also documented and designed to be repeatable. This simple formula is the key to intelligence-based security; apply it where you need a formula for factual intelligence-based decision making.

ITEBOOKS.DIRECTORY

22

Other Examples of Execution

The following examples are plans from a company separate from the electrical utility company, which provided the majority of examples used in this book. The following assessment and implementation plan was at a large company that had initiated an "intelligence" program but was limited by several factors. First and foremost were a lack of understanding on what constituted an intelligence program and lack of adequate personnel, training, and resources. The assessment identifies the issues and the implementation plan is a combination of both strategic and tactical planning:

Intelligence Program Assessment Enterprise September 4, 2014

This is an assessment of the intelligence program for an enterprise that consists of 15 major facility locations in 10 states with approximately 5,000 employees across the nation. There are numerous other support resources owned by the enterprise; also, thousands of contractors work at enterprise facilities across the United States.

Corporate Security has responsibility for the physical security of assets/personnel across the enterprise. The security program management is the responsibility of the senior director of Corporate Security, who is stationed at one of the largest facilities but not at corporate headquarters. Site security is the responsibility of each site, and security operations vary by location. Security officers from contract security have contract responsibilities for sites enterprise-wide through a national contract recently implemented.

For example, at another major campus, security operations function 24 hours a day, 7 days a week, and consist of a cadre (55) of

ITEBOOKS.DIRECTORY

security officers, including supervisory security officers, a command center, executive desk posts, truck gate posts, vehicle patrols, foot patrols, and fire safety officers. The campus also has responsibility for the Business Intelligence Operations Center (BIOC), which was established to monitor open-source reporting for information that may have an impact on enterprise operations.

On September 4, 2014, an assessment was initiated by the security team at this large campus along with the investigations manager; it was a collaborative effort between the security staff designed to evaluate, analyze, document, and make recommendations for improvement of the intelligence program.

OBJECTIVES

The overall mission/objective is to analyze, evaluate, organize, and recommend intelligence program options for operations across the Corporate Security field of responsibility: define an intelligence program and implement authorized elements of the intelligence program, then engage the entire security team and train them regarding the developed intelligence program standards.

CURRENT STATE

The BIOC took the initial steps of the enterprise intelligence program and is frankly the only current element of an intelligence program at Corporate Security. The BIOC has a mission statement as follows: The goal is to proactively monitor, gather, analyze, and document several open data resources providing information on current news, weather, direct communications (phone calls), and media-related issues that could have an impact on or damage enterprise intellectual and physical assets and to serve as the central information-gathering, dissemination, and travel assistance center for enterprise North American operations.

The BIOC has three elements to its mission:

1. Traveler's assistance center.
2. Analysis of open-source data and internal communications for information that may have an impact on enterprise operations.
3. Communicate pertinent information to the proper resources/outlets.

Since its inception approximately two years ago, the BIOC has been struggling to meet its mission objectives. There have been issues with the traveler's assistance center, including the notification alerts to persons who were not traveling, usually due to cancelled trips or

ITEBOOKS.DIRECTORY

administrative assistants who made reservations for executives but did not travel themselves. Sometimes, the notifications came days after the events or were difficult to understand.

There have also been issues with the analysis and reporting of intelligence information from the BIOC officers. Many do not understand the BIOC mission, which is generally defined and open to interpretation. The officers staffing the BIOC have not received training specific to their analytic duties and are security officers, not experienced analysts. The reporting element has also been spotty and problematic, again going back to the training issue. The August 15, 2014, transition of contract security companies with a high turnover of personnel has also negatively impacted BIOC operations.

The issues are highlighted as follows:

1. General mission/objectives
2. Security officers in analyst positions
3. Lack of training

One avenue to consider is companies that provide analytical services specific to open-source reporting and social media regarding a business impact that may fit the needs of the enterprise. These companies provide the analytical services on a monthly fee basis but will also provide training specific to data analysis and reporting to enterprise personnel. If so engaged, it would allow the BIOC to report information compiled by the analytical company. The current duties of the BIOC could be divided, if the utilization of the analytical company is cost effective.

INTELLIGENCE PROGRAM AREAS FOR FUTURE CONSIDERATION

In addition to the BIOC, there are other missions/objectives to consider for inclusion in establishing an intelligence program at the enterprise. These elements are essential to a robust intelligence program, but a staggered implementation is recommended as a practical and cost-efficient method to allow for evaluating and measuring the success of each phase of the program. The elements are defined next:

1. **Vulnerability Assessments:** Are designed to assess physical vulnerabilities and to implement mitigations of enterprise assets and facilities to reduce vulnerabilities.
2. **External Threats:** Specific individuals or organizations are identified as potential threats; analysis includes potential adverse actions from these threats, which are measured and mitigated.

ITEBOOKS.DIRECTORY

3. **Insider Threats:** A malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors, or business associates, who have inside information concerning the organization's most valued assets; analysis includes potential adverse actions from these threats, which are measured and mitigated.
4. **"Blended" Physical and Cyber Security:** Assess and defend against the cyber-led attacks intended to defeat physical security measures or the physical-led attack designed to gain access to cyberassets.
5. **Risk Assessments:** The identification, evaluation, and analysis of the levels of risks regarding a company's assets and levels of protection, their comparison against standards, and determination of an acceptable level of risk.

More detailed description of the aforementioned intelligence program is as follows:

VULNERABILITY ASSESSMENTS

The vulnerability assessment is designed to assess all mitigations to vulnerabilities from any possible threat, whether human made or from nature. The assessment should consider possible attacks on facilities, assets, and personnel. The parameters measured in a vulnerability assessment should include identifying company vulnerabilities, reviewing current practices and preparedness, and then developing an action plan to mitigate identified vulnerabilities. As security or intelligence personnel are not often experts in all aspects of a company's most valuable assets, appropriate company departments should be engaged to conduct vulnerability assessments of the equipment critical to operations throughout the company. Security and engaged departments should work together to conduct site-specific vulnerability assessments of company facilities and critical assets. The results of the vulnerability assessments should be documented, along with mitigation steps, and be revised annually or as assets change through the assessed facility.

EXTERNAL THREATS

Several enterprise departments have regular interaction with the public while carrying out their regular daily duties. During some of these interactions, incidents may occur that cause concern for employee safety. These concerns generally materialize from face-to-face interactions, phone calls, or e-mails or letters that contain some type of

ITEBOOKS.DIRECTORY

concerning communication expressing dissatisfaction with the company. These departments have handled these issues with no formal means of documenting incidents for future reference or referral. The same individual may have several contacts with company personnel at different sites, with escalating levels of behavior that may become explosive. Without methods for tracking and measuring people who are deemed threats, the explosive behavior appears to come out of nowhere until postincident investigation reveals the prior behavior and contacts with company personnel.

To address the problem, it is recommended Security conduct a company-wide assessment to gather information about anyone who made direct threats to the company. For each threat made, Security should conduct interviews with company personnel who witnessed the incident. Security will then further investigate to determine whether this person had made previous threats or had a history of violence. In evaluating potential external threats, Security must evaluate capability and intent. An individual or group threat highly capable of an attack can develop the intent to attack the organization quickly. However, those with high intent and low capability will require time to develop the capability to cause damage. Security should develop the tools to monitor the intent and capability of known threats.

If the investigation revealed that a person might be a threat, Security should create flyers for company employees. The flyers should contain specific information about the person, such as their address and the threatening actions he or she had taken against company personnel. Security should distribute these flyers to each office building and to each department that might have contact with the potentially dangerous individual. This information should be placed on a shared computer drive for all company personnel to access. The implementation process overview is synopsized as follows:

1. The External Threats Intelligence Program consists of Corporate Security gathering information on potential threats to the enterprise and entering this information into a central database.
2. Once the information has been received, Corporate Security analyzes the information, evaluates the threat, and makes a determination as to the risk the threat poses for the organization and its personnel.
3. This process provides a means for all external threats to be analyzed, evaluated, and prioritized.
4. Once a level of concern has been established, Corporate Security then disseminates the information to appropriate departments in an effort to protect enterprise assets.

ITEBOOKS.DIRECTORY

INSIDER THREATS

An *insider threat* is a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors, or business associates, who have inside information concerning the organization's physical and cybersecurity practices, data, or computer and physical access systems. The threat may involve fraud, the theft of confidential or commercially valuable information, the theft of intellectual property, damage to company assets, physical harm to personnel, or sabotage of computer systems. The implementation process overview is as follows:

1. Consideration should be given to the formation of a collaborative enterprise Insider Threat Working Group with members from Security, Human Resources, Legal, and other departments (as deemed appropriate). Individuals are dedicated to developing into a structured, focused, and organized team with a clearly defined mission that provides valuable protective services to the enterprise and its employees.
2. Initiate an assessment of the insider threat risk at the enterprise. Enterprise employees are the company's greatest asset, but they are also the company's greatest risk. The initial assessment should concentrate on developing a capabilities matrix related to positions throughout the enterprise.
3. The assessment should expand to developing the ability of the team to evaluate situations. An example is a personal crisis; personnel or contractors may develop personal situations that could possibly devolve into malicious intent; their activities and capabilities to potentially harm the enterprise should be monitored until the situation is resolved.
4. Initiate monthly or as-needed meetings of the Insider Threat Working Group to handle situations.

BLENDED PHYSICAL/CYBER SECURITY

It has become apparent in the modern world that Physical and Cyber Security Departments must coordinate security efforts between departments dealing in the physical and cyber arenas. The coordinated attack of a threat on both physical and cyber systems is of great concern. The goal of the security collaboration is to assess and defend against the cyber-led attack that defeats physical security measures or the physical-led attack designed to gain access to cyberassets. Physical Security and Cyber Security should evaluate the possibility of developing collaborative assessment tools and in the future developing collaborative incident response plans.

ITEBOOKS.DIRECTORY

1. Coordinated attack (physical and cyber). Assess and defend against the cyber-led attack that defeats physical security measures or the physical-led attack designed to gain access to cyberassets.
2. Develop collaborative assessment tools. Develop collaborative incident response plans, including, but not limited to, the following threats:
   a. Insider threat: disgruntled employee/contractor
   b. External threat: terrorist, disgruntled landowner, or organized lone wolf
   c. State-sponsored attacks
3. Evaluate the value/necessity of reporting to one centralized chain of command.

RISK ASSESSMENTS

Risk assessments involve the identification, evaluation, and analysis of the levels of risks regarding a company's assets and levels of protection, their comparison against standards, and determination of an acceptable level of risk. The mitigation of the areas listed previously led to the measurement of how much risk the enterprise is willing to accept for gaps identified in the compiled assessments. Risk assessments would be the final component to the intelligence program, allowing executives to determine under what level of risk they are willing to operate.

1. Make a comprehensive overview of all aforementioned intelligence program components.
   a. List assets and level of protection.
   b. List methods for risk reduction.
   c. Summarize levels of risk, what are in place versus what is needed.
   d. Make recommendations and suggestions for executive decisions regarding risk management.

RECOMMENDATIONS

Based upon the analysis, the following are recommendations for improvement:

- Conduct and document a collaborative assessment of current enterprise intelligence program security operations. Concentrate on identifying gaps and make recommendations in areas of opportunity for improvement.

ITEBOOKS.DIRECTORY

- Define the BIOC mission/objectives.
  1. Consider hiring an analytically capable company to meet mission/objectives.
  2. Hire better-qualified candidates for the BIOC.
  3. Write/revise BIOC post orders as a foundation of standardized operations.
     a. Analyze post assignments for additional documentation related to specific post assignments.
  4. Train the BIOC personnel to defined standards.
- Develop the intelligence program to include the following:
  1. Appoint an intelligence program manager.
  2. Hire a senior analyst or engage a contract company to assist in the implementation.
  3. Develop a 3- to 5-year staggered strategic implementation plan.
  4. Hire qualified analysts capable of conducting the following:
     a. Vulnerability assessments
     b. External threat assessments
     c. Insider threat assessments
     d. Cyber-/physical security collaboration
     e. Risk assessments
- Maintain the intelligence program.
  a. Pilot programs to test value
  b. Annual assessments
  c. Management oversight
- Develop a "culture of intelligence."
  a. Coordinate with Corporate Communications to develop an intelligence awareness campaign.

With the assessment completed and identification of the lack of components of an intelligence program, the following are documented solutions for the enterprise to consider to implement for developing an intelligence program:

Intelligence Program Implementation Plan (1–3 Years)

SHORT TERM (12–18 MONTHS)

- Conduct and document a collaborative assessment of current enterprise intelligence program security operations. Concentrate on identifying gaps and make recommendations in areas of opportunity for improvement. (Complete by September 30, 2014.)

ITEBOOKS.DIRECTORY

- Analyze, evaluate, and make recommendations for a robust, user-friendly, searchable data management system to sustain and complement future intelligence/investigative missions/objectives and daily operations. (Complete by December 31, 2014.)
- Stabilize and standardize BIOC operations.
  1. Define the BIOC mission/objectives. (Complete by December 31, 2014.)
  2. Analyze post assignments for additional documentation related to specific post assignment. (Complete by December 31, 2014.)
  3. Write/revise BIOC post orders as a foundation of standardized operations. (Complete by March 1, 2015.)
  4. Hire better-qualified candidates for the BIOC. (Complete by June 1, 2015.)
  5. Train the BIOC personnel to defined standards. (Complete by September 1, 2015.)

LONG TERM (12–36 MONTHS)

- Develop the intelligence program to include the following:
  1. Pilot programs to test value through an implementation plan. (Complete by September 30, 2014.)
  2. Develop a 1- to 3-year staggered strategic implementation plan. (Complete by September 30, 2014.)
  3. Appoint an enterprise intelligence program manager. (Complete by December 31, 2014.)
  4. Hire a senior analyst or engage a contract company to assist in the implementation. (Complete by December 31, 2014.)
  5. Hire a qualified cadre of analysts capable of conducting the following components (a specific plan should be developed for each):
     a. External threats (complete by February 1, 2015)
     b. Vulnerability assessments (complete by April 1, 2015)
     c. Cyber/Physical Security collaboration (complete by July 1, 2015)
     d. Insider threats (complete by December 1, 2015)
     e. Risk assessments (complete by February 1, 2016)
- Maintain the intelligence program. (Complete by February 1, 2017.)
  a. Annual assessments
  b. Management oversight

ITEBOOKS.DIRECTORY

- Develop a culture of intelligence. (Complete by September 1, 2017.)
  a. Coordinate with Corporate Communications to develop an Intelligence Awareness Campaign

The enterprise did see the value of the intelligence program from the documents listed. The following plan was implemented to train the BIOC officers in the five core missions identified for them. It also was meant to initiate and set the external "known" threats program as the cornerstone of the intelligence program at the enterprise.

BIOC Officer Training Program Training Objectives

The purpose of this block of instruction is to clearly define the roles, responsibilities, and daily duties of the Business Intelligence Operations Center (BIOC) and train current contract security BIOC officers to accomplish their core missions. It is also intended to develop a repeatable process to be utilized in the training of future BIOC officers.

CORE BIOC MISSIONS

The five core missions of the BIOC are:

1. Intelligence: Intelligence involves the gathering, analysis, and dissemination of data pertaining to the national enterprise. The intelligence component will include the initiation of an external threats program, with analytical products generic to known external threats.
2. Traveler's assistance: This mission is to track enterprise travelers located worldwide and to effectively track/analyze natural and/or human-made incidents, emergencies, weather-related events, natural disasters, pandemics, or acts of violence that may affect the traveler and effectively communicate the event to the affected traveler for awareness and preventive action.
3. Camera tours: Enterprise security camera systems will be utilized to tour the campus through video surveillance and report any suspicious activity to patrol officers for further investigation and resolution. When completed, document the camera tours in the daily log.
4. Incidents: Assist the dispatch officer in an incident/emergency. Answer routine telephone calls and routine requests and log all activity in the daily log.
5. Communication: Each of the BIOC core missions is dependent on effective, efficient, and timely communication systems and BIOC officer execution according to standard procedures.

ITEBOOKS.DIRECTORY

TRAINING OUTLINE

An analysis was conducted to determine the BIOC core missions as stated previously. It has been anticipated that a two-hour block of instruction to all BIOC personnel will be sufficient to train and evaluate the capability of current BIOC officers. Follow-up will include the standardization of procedures, processes, and guidelines in a BIOC post order binder and its inclusion in a manual of operations. The following is a proposed agenda for a three-hour block of BIOC officer training; it is anticipated the training will be scheduled and conducted during the week of November 17, 2014.

Agenda

Prework: Read the September 2014 *Security Management* magazine article "Let Intelligence Light the Way."

First hour: Traveler's assistance program and communications

- Overview of the BCD Travel Database
  - Utilization
  - Reporting
- Available data for traveler risk analysis
- Review of communication processes/flip charts
- Mechanics of reporting/communications

Second hour: Camera tours, incidents, and communications

- Camera tours
  - Utilization of cameras to conduct a virtual video patrol of the campus
  - Response to any suspicious activity
    - Dispatch patrol officer with actionable information
  - Logging camera tour in iTrack
- Incidents/emergencies
  - Assist the dispatch officer in appropriate situation
    - Incident/emergency
- Answer routine telephone calls
- Address routine requests
- Fire panel notifications
- Daily log updates in iTrack
- Review of communications
  - iTrack
  - Send word now
  - Traveler's assistance
  - Radio/Direct connect communication

ITEBOOKS.DIRECTORY

Third hour: Intelligence program and communications

- Overview of intelligence program
- Demonstration of analysis of known (external) threat subject
  - Compilation of analysis into standard format
  - Entry of data into Excel spreadsheet as a database
- Dissemination of known threat subject information to security team
- Demonstration of real-time analysis of subject information
- Future applications of analytical capabilities

As you can see, the methodology that was used at the electrical utility company was applicable to this environment as well. Completing the initial assessment at the second company was not difficult as this company did not track any of the information relating to insider or external threats. The company did not conduct comprehensive vulnerability assessments that involved their Corporate Security members, instead calling in third-party vendors and then classifying the reports as "privileged and confidential."

The challenges to effectively communicate the benefits of a robust intelligence program to this enterprise are to find areas where success can be documented and metrics can be tracked (Figure 22.1). At the utility company, it was the copper theft initiative; at this enterprise, it was the establishment of the BIOC as a center with true intelligence analytical and reporting capabilities.

As you can see, the establishment of the BIOC known threat program was meant to be the establishment of an external threats program; it was also to be the cornerstone of the intelligence program. The enterprise had collected data on known offenders who had been arrested on one of their largest campuses, but the information was sporadic and kept in myriad files and formats. The establishment of a formal, standard form for tracking known threats and a database on a SharePoint site along with the training of BIOC officers to track and analyze data through the known offender threats program allowed us to develop their analytical thinking. This led to the establishment of a truly intelligence-based security posture that would open the doors to other intelligence-based objectives.

The BIOC training was presented and the level of engagement by the contract officers varied from true engagement, as evidenced from persons asking legitimate questions and taking notes; to officers asking about how much more work they would be doing; to veiled disinterest, as evidenced by yawning and difficulty staying awake.

ITEBOOKS.DIRECTORY

There was an assignment handed down to the BIOC officers to gather available data and conduct a thorough analysis of 36 people who had been documented as known offenders because they had either been arrested or been cited by the police for trespassing, panhandling, or other general misdemeanors relating to the enterprise. There were 16 people included in this group who had been implicated in a rash of car burglaries that included crimes on the enterprise property.

The problem with the past practices was the data were kept in myriad paperwork depending on who was documenting the threats at the time they were handled. There was no way to re-create any contacts with subjects who were not documented.

The assignment was to conduct the analysis of the people the officers were assigned and compile a standardized flyer on each of the subjects using a standardized format, with the goal to initiate a known threats program with standardized and repeatable processes. The format included a subject photograph and a general physical description of the subject, including date of birth, age, race, gender, height, weight, hair color, and eye color. The flyer also would include a narrative that described the subject's involvement with the enterprise and a section on past criminal history, which also included any officer warning and law enforcement intelligence. The following are examples of the narrative and criminal history sections:

> **Narrative:** On September 16, 2014, subject [name] and accomplice [name and date of birth] were trespassing on enterprise property on two separate occasions. The first incident occurred at approximately 13:35, resulting in officers following the subjects off the property. The second incident occurred at approximately 16:35; in this incident, both subjects were stopping cars and asking for money on XXth Street and State Street. This incident resulted in the arrest of both subjects for trespassing by Police Department bike and patrol officers. These subjects are to be handled with caution in any future contacts as both have criminal records.
>
> **Criminal activity:** Subject was arrested for trespassing in regard to the September 16, 2014, incident on enterprise property. Subject has a lengthy criminal record, with convictions in 2008 (retail theft); 2005 (criminal damage to property); 2003 (resisting/obstructing an officer); and 1998 (criminal trespass and theft). Other intelligence indicates that subject runs a "crack" house on XXth Street in an apartment (106).

ITEBOOKS.DIRECTORY

Further investigation into these 36 subjects revealed past criminal histories that included serious violent crimes. It was determined that, of the 36 subjects who were known to the enterprise, 15 (42%) of them had serious felony charges, such as those for armed robbery, robbery, battery, arson, drug charges, carrying a concealed weapon, felon in possession of a firearm, burglary, prostitution, resisting/obstructing a police officer, and sex offenses. Until the BIOC training class, these charges were unknown to the enterprise or the contract security company.

This raises the point of "knowing your enemy"; without the additional criminal history information, security officers are sent into a situation with potentially dangerous felons armed only with information that the subjects they are contacting are former "trespassers." However, with a robust known offenders program, the responding security officer should have a binder of known offenders at their disposal. The officer has the ability to look up information on people they know are familiar and be more informed and better prepared to either contact the subject or watch from a distance while dispatch calls the police.

The more information you have on the subject that you already know, the more prepared your officers will be when they approach these subjects. The format we developed to track the known offenders was a standardized template for a flyer; we included the information on each of the subjects in an Excel spreadsheet. Once the training was completed and the BIOC officers had completed their assignments, we ensured the process was repeatable when other subjects who showed up on campus were identified as threats.

This was to be the cornerstone of the intelligence program at the enterprise. Unfortunately, I left the enterprise to pursue other endeavors prior to completion of the intelligence program process.

ITEBOOKS.DIRECTORY

23

Follow-Up

The vision I had for this book was to develop a guide for people who wanted to set up an intelligence-based security posture in their private corporate security departments. The purpose was twofold: One was an educational track that would show the benefits to the Corporate Security Department that I was leading, and the other was to provide something people could read and refer to regarding how to identify their specific threats and the threats' capabilities, allowing them to develop a security program that would benefit from this material and put measures in place to protect their people and assets. After 28 years in law enforcement, I consider myself a "true believer"; I wanted to assist those out there who might not have the same background and exposure to the benefits of applying a robust intelligence program in their company.

To be honest, I have been surprised by the slow response to developing a system that bolsters the security posture in a company; the system provides the potential to save money through effective and efficient operations. The future of private security will depend on security professionals who enhance their departments by conducting an analysis of past incidents, law enforcement records, demographics, crime statistics, industry history, presence of criminal or terrorist organizations, direct external threats, and internal threats along with evaluating present security operations to propose cost-efficient security improvements to provide satisfactory levels of risk acceptance to the evaluated enterprise. As detailed throughout this work, the advantages of knowing who your adversary is and what capabilities the adversary has to bring to bear against your organization allows you to plan and prepare accordingly.

ITEBOOKS.DIRECTORY

The more specific the threat streams, the more specific the preparations to mitigate risk will need to be. The reality is that even if you have the best security and intelligence program in the world, there will be breaches in security at your organization. The vulnerability assessments will mitigate risk, but a tornado still has the ability to cause significant damage to critical assets. However, resiliency is a key component to the risk assessment; in your company, if you can ensure that by aligning resources in preparation for a disaster, when the disaster comes, everyone will know what to do and how to do it and maintain operations when your competitors are shut down by the events, waiting for the Federal Emergency Management Association (FEMA) or the U.S. government to assist them.

Finally, there is the need to maintain the intelligence-based security program. It is a lot of work to set up such a program; however, there are expiration dates on all intelligence. It is necessary that you conduct annual risk assessments of evolving intelligence threat streams. Continue to coordinate and share intelligence with aligned industry partners. Maintain and expand liaison contacts in appropriate arenas. Document efforts and develop standard operating procedures to track and monitor the ever-changing threat streams and establish a status board of priorities. Set up the incident response teams and emergency crisis teams and practice scenarios with them. Ensure they have the tools to operate in a crisis, either natural or human-made.

Most important, track success and keep your organization informed of the value of the intelligence-based security program, build a good team, take care of the team, and allow them to help you build to the success that you know you are capable of attaining.

ITEBOOKS.DIRECTORY

INDEX

ITEBOOKS.DIRECTORY

C

ITEBOOKS.DIRECTORY

ITEBOOKS.DIRECTORY

ITEBOOKS.DIRECTORY

ITEBOOKS.DIRECTORY

ITEBOOKS.DIRECTORY

ITEBOOKS.DIRECTORY

ITEBOOKS.DIRECTORY

ITEBOOKS.DIRECTORY