



ENTERPRISE  
SECURITY  
— FOR THE —  
EXECUTIVE

SETTING THE TONE  
FROM THE TOP

Jennifer L. Bayuk

Foreword by Donald F. Donahue

*This page intentionally left blank*

---

# ENTERPRISE SECURITY FOR THE EXECUTIVE

---

---

## SETTING THE TONE FROM THE TOP

---

Jennifer L. Bayuk

Foreword by Donald F. Donahue

**PRAEGER**

*An Imprint of ABC-CLIO, LLC*

A B C  C L I O

Santa Barbara, California • Denver, Colorado • Oxford, England

Copyright 2010 by Jennifer L. Bayuk

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, except for the inclusion of brief quotations in a review, without prior permission in writing from the publisher.

### **Library of Congress Cataloging-in-Publication Data**

Bayuk, Jennifer L.

Enterprise security for the executive : setting the tone from the top / Jennifer L. Bayuk ; foreword by Donald F. Donahue.

p. cm.

Includes bibliographical references and index.

ISBN 978-0-313-37660-3 (hbk. : alk. paper) — ISBN 978-0-313-37661-0 (ebook)

1. Business enterprises—Security measures. 2. Business enterprises—Computer networks—Security measures. 3. Computer security—Management. 4. Data protection—Management. I. Title.

HD61.5.B39 2010

658.47—dc22

2009039314

14 13 12 11 10 1 2 3 4 5

This book is also available on the World Wide Web as an eBook.

Visit [www.abc-clio.com](http://www.abc-clio.com) for details.


Praeger

An Imprint of ABC-CLIO, LLC

ABC-CLIO, LLC

130 Cremona Drive, P.O. Box 1911

Santa Barbara, California 93116-1911

This book is printed on acid-free paper 

Manufactured in the United States of America

# CONTENTS

<i>Foreword by Donald F. Donahue</i>	<i>vii</i>
<i>Acknowledgments</i>	<i>xi</i>
Introduction	1
1. Tone at the Top	9
2. Threats and Vulnerabilities	23
3. Triad and True	37
4. Secure Products and Services	61
5. Security through Matrix Management	77
6. Navigating the Regulatory Landscape	93
7. Investigation and Remediation	107
8. The Right Stuff	119
Conclusion	131
<i>Appendix: Case Study</i>	<i>133</i>
<i>Notes</i>	<i>153</i>
<i>Index</i>	<i>161</i>

*This page intentionally left blank*

# FOREWORD

At the dawn of the twenty-first century, the issue of “security” for businesses and individuals came roaring in as the concern of highest importance. For many of us, the peaceful confidence that security, as a personal or as a corporate matter, had faded as a priority brutally burst with the sights of the morning of September 11, 2001. Life has not been the same since. Yet, for business and corporate leaders, this peaceful confidence had always been an illusion. Security remained, and remains, a top priority for businesses, and the challenges of ensuring that our companies could operate securely and safely have only grown in recent years.

Today, meeting those challenges poses unique demands on businesses and on business leaders. The days when it was enough to have a lone security guard rattling doors to check their locks are long gone; now, the doors are often virtual, the locks easily undone through careless action by an ill-informed individual. As the technology and processes that support our businesses become ever more sophisticated, security requires a much higher level of awareness much more broadly within the organization. It also requires leadership at all levels of the organization to cultivate and embed a consciousness of how to act securely—a “security mindset”—throughout the organization.

Every organization is led by a collective of individual leaders at different levels throughout the organization. Each leader’s “following” must behave securely in order to secure the whole. And that same interdependency is reflected throughout the nation. As each organization or each com-

munity looks to its own leaders for direction on behavior, the security of our nation depends to a great extent on the degree to which each leader can influence security-related behavior in his or her own environment.

My company, DTCC, is the backbone of the nation's securities markets, providing services to complete securities trades and to handle securities assets (processing dividend payments and the like). In 2008, DTCC handled about \$1.9 quadrillion worth of securities transactions on behalf of its members and the U.S. investing public. It is our job to provide certainty in a landscape scoured by storm. For us, the sheer value of the transactions we process and the trust our members and their investor clients place in us to handle their financial activities safely make security the highest priority. "Safety and soundness" is the bedrock of our operation, and the first and last test of how effectively we are meeting our customers' needs.

But through experience we've learned that "safety and soundness" is not something we can control by ourselves—it requires us to work collaboratively with our financial institution members to promote the safety, soundness, and security of our financial "community." For that reason, I was honored to chair the *Financial Services Sector Coordinating Council* (FSSCC) for Critical Infrastructure Protection and Homeland Security from 2004 through 2006. The FSSCC is a group of more than 30 private sector firms and financial trade associations that work with the Department of Treasury to help reinforce the financial services sector's resilience against terrorist attacks and other threats to the nation's financial infrastructure. The mission of the FSSCC is to foster and facilitate the coordination of financial services sector-wide voluntary activities and initiatives designed to improve critical infrastructure protection and homeland security.

The FSSCC leadership experience was both challenging and rewarding. The challenges ran the gamut—from the nuts and bolts of working with government officials and private sector representatives to restore financial services to those affected by Hurricane Katrina, to the high-level issues of strategizing how to respond to new threats to the nation's information technology infrastructure. But consistent in all of these challenges was a very clear message as to how my actions as the CEO of my company affect the security-related behavior of people, processes, and technology in areas that I would not previously have imagined.

Among the rewards was the pleasure of working with so many committed financial services professionals, each of whom was dedicated to addressing security issues as they affected the financial infrastructure of the nation. One of these was Jennifer Bayuk, the author of this book, who very successfully took on the daunting task of establishing an FSSCC



workgroup to coordinate “research and development” on security matters for the financial services industry. In a highly complex area, Jennifer and the FSSCC R&D group struck a remarkable balance between practicality and leading-edge innovation, providing significant guidance to researchers on how to progress the key security issues for financial services.

At the time, Jennifer was the chief information security officer for Bear Stearns & Co., a major investment bank later brought down by the impact of the credit crisis of 2007–08. Despite the fall of Bear Stearns, the security perimeter that Jennifer enforced on her watch there was one of the most respected on Wall Street. She exemplifies tone at the top when it comes to security, and any leader who wishes to have influence in that arena would do well to read this book.

Donald F. Donahue  
Chairman & Chief Executive Officer  
The Depository Trust & Clearing Corporation

*This page intentionally left blank*

# ACKNOWLEDGMENTS

I am indebted to two security luminaries who volunteered their perspective on early drafts, with the result that this book is consistent with a background of experience much wider than my own. Thank you, Eric Guerrino and Donn Parker. Many other practitioners have shared their security horror stories over the years, for which the profession as a whole will be grateful. I must also thank Nancy S. Lee for her ingenuity in illustrating security lessons in a method that allows them to be intuitively grasped by those outside the security profession, and with humor that many in the profession would not have believed possible. I also acknowledge with pleasure my most critical reviewer, without whose support this book would not be possible, Michael Bayuk.

*This page intentionally left blank*

# INTRODUCTION

This is not a book about security management; it is a book about security leadership. It is a book for business leaders in all domains. Most leaders are somewhat concerned about security, and many do not know what to do about it. This book is for them. It takes the mystery out of business security functions. It describes what an executive needs to know in order to influence how security works in the organization, without getting into the detail needed to manage it directly.

I use the term *CXO* to refer to executives high enough on the organization chart to merit an undisputed “Chief” in their title. A *CXO* is the only one in his or her job function at his or her level; examples are chief executive officer, chief financial officer, and chief operating officer. Business unit presidents fall into this category, as does any other manager with enough clout to set organization-wide levels for risk tolerance. In dozens of coffee breaks, luncheons, and cocktail hours for the past six months or so, I have been asking my peers in the security profession this question: “What do you say to *CXOs* to help them understand security?” The answer was nearly universal: “Tell them a horror story. *Fear, uncertainty, and doubt sell security.*” The fact is so well known that *security horror story* is a well-defined tool of the trade. An Internet search on the term will lead you to sites frequented by security professionals. A security horror story is a tale of a company that did not pay attention to security and thus fell victim to some criminal who exploited an obvious vulnerability to steal or

destroy something so valuable that the company had to disclose its inadequacy. The inadequacy could be disclosed by calling law enforcement, by declaring a loss on financial statements, or, in the worst case, by going out of business.

Given the nearly unanimous response to my informal survey, it is unlikely that a CXO will have ever seen a presentation on a reasonable approach to provide basic security measures outside of an atmosphere designed to produce fear, uncertainty, and doubt. The fact that security horror stories work to sell security is so widely known that security-product salespeople call it the “FUD factor.” A FUD factor is the level of fear, uncertainty, and doubt that the audience for a security horror story feels upon hearing it. The premise is that when people experience FUD—really experience it—they are motivated to improve security posture. Where a CXO has experienced a security incident that caused harm to his or her own company, a security horror story is not needed, but the FUD factor is assumed to be working especially well in favor of security spending. Security professionals understand that they get full and undiluted CXO support primarily after a major security breach happens on that CXO's watch, or to a very similar competitor.

Be that as it may, most CXOs I know don't really believe security horror stories will happen on their watch. CXOs typically work in environments where things generally appear to be always under control because they have their own hands on the helm. They have experienced major obstacles in their careers, and there is rarely a threatened event that fazes them. They rightly place market risk and credit risk above operations risk, and security risk is a subset of operations risk. Where information technology is a risk, as much damage can be caused from its working incorrectly or not at all as from its being maliciously attacked. When my boss at Bear Stearns introduced me to then-CEO Jimmy Cayne, saying, “Meet our chief information security officer,” Jimmy's reaction was puzzled and swift: “We have a what?” It had never occurred to him, as it does not at most firms, that it was necessary to have a CXO dedicated to security.

So despite popular opinion among security professionals, I was never a true believer in FUD. Perhaps it is because I worked on Wall Street, where, as one veteran put it, “They relish it. Live for it. Eat it for breakfast. Risk is what drives these people.”<sup>1</sup> Managers rose in the ranks precisely because they were not afraid of anything. They instinctively challenged anyone who suggested they were taking too much risk. Nevertheless, I do agree with my peers that CXOs are motivated to spend on security in response to an incident. But the motivation is not necessarily FUD. In my observation, it has

been a prudent due diligence. A CXO does not want to be the one to miss a clear signal that something bad may occur. Even risk-taking CXOs don't want to see a security breach on their watch. And security measures are relatively cheap. (Security professionals might not think so, but CXOs are comparing them to business enablers that cost 100 times more.) Taking the advice of a security professional in a time of crisis is like buying insurance.

Unfortunately, many CXOs who have spent heavily on security specifically to avert security incidents have been misled. There are so many security products and services out there that it is rare when the one recommended as a panacea in a crisis is the right long-term solution to protect the business from further exploit. The result is that many executives see security as just one long spending pattern with no end in sight, and they see little added value as the incidents pile up despite the constant spending. It is well documented that spending on security does not necessarily make one more secure.<sup>2</sup> The benefits of one expensive security *strategy* as opposed to another, on the other hand, are not very well documented. At the CXO level, this starts to become frustrating, and so it is common for firmwide Security Programs to be revisited and reorganized every few years.

Here is an example of the FUD-factor scenario played out among security departments, CXOs, and security vendors. A large institution had a huge problem with Social Security- and credit card-number theft, and corresponding identity theft. The security group investigated some incidents and found a few cases where business operations used unsecure methods of sending and receiving personally identifiable information via the Internet. They spoke with their peers at other organizations and were introduced to a set of security product vendors, who advised them to set up network listening devices between their internal network and everywhere it touched the Internet. The security department reported the incidents to their CXO and described a technology solution that would cost about \$5 million. The CXO agreed to implementation. A vendor was chosen. The money was spent, and the system installed. Then the security group consulted the legal department for a procedure on what they should do when the devices produced reports that credit card and Social Security data was leaving the firm. The legal department told them that they should automatically stop the transmission of the data. However, the equipment that the security group installed could only report that information was leaving the firm; it could not stop the transmission. To change the technology to be able to stop data from leaving the firm would cost an additional \$8 million or so. The legal department was aghast that nowhere in the security department's proj-

ect plan was there any coordination with the departments who actually were using the data; it told them to turn off the reporting technology, because otherwise the company would be legally required to act on known violations of the law, and there was no procedure for doing that. The security group applied to the CXO for an \$8 million budget increase to add technology to prevent the data from leaving the firm, calling it “a last-minute legal requirement.” They did not get the funds, because when the CXO discovered this folly, all new security projects were put on hold pending security department reorganization.

From the point of view of security product vendors and the (perhaps unwittingly complicit) security group, the fact that data was leaving the firm was used to create the FUD that motivated spending on a good first step, and the spending should have continued until the problem was solved. From the point of view of the CXO, the “insurance policy” was a scam and there was no reason to throw good money after bad. This is a typical example of why many CXOs are now immune to FUD as a method to sell security. They gave the security department the benefit of the doubt to come up with solutions that would solve a business problem, while the security department was instead concentrating on projects to implement one type of security technology.

The recurring theme in these scenarios motivates CXOs to demand more insight into the security solutions presented to them. CXOs are also often motivated by the belief that reasonable security should cost less than currently budgeted amounts. There is no doubt that some spending is necessary. But more CXO-level insight into return on investment with respect to security measures is needed in order to gain better control over security decisions. This obvious requirement has produced a wave of literature on the costs versus benefits of security spending. Very sophisticated economic arguments that were originally developed to assist decision making with respect to all sorts of business spending have been rigorously applied to security projects.<sup>3</sup> A simplified version of all these arguments goes like this: (1) start with the probability of an event that could cause harm; (2) multiply that probability by a cost figure of expected losses that may result from the event; (3) compare the product to the amount one would have to spend to make the company secure.

1.  $P$  = probability of event that causes harm  
 $C$  = cost of damage from the event  
 $T$  = cost of technology to prevent harm
2.  $P \times C$  = amount it is reasonable to spend to prevent the event
3. If  $(T < P \times C)$ , buy  $T$



The problem with these approaches is that  $P$  will always be an estimate that varies with the organization's attitude toward risk. Any calculations based on such an approach are thus completely subjective. There is also the *Black Swan* argument, which says that, because no one can predict which completely unanticipated events are even possible, there is no way to estimate  $P$  at all.<sup>4</sup> There is also, in my opinion, the “elephant in the room” argument. It is the issue looming so large that people are obviously aware of it even if no one brings it up: *Is T the most appropriate method of reducing C? Might there be alternatives that have not yet been considered? As Warren Buffett, albeit in a different context, put it, “Our advice: Beware of geeks bearing formulas.”*<sup>5</sup>

Another common approach to decisions with respect to security is the *best-practice* approach. In this view, the fact that others in the same industry have decided to implement a certain type of security measure provides a good reason to adopt it internally. Though a lot of good standards documents have been written in the name of best practice and should by no means be disregarded as an important source of professional literature, there is a variation on the best-practice theme when it comes to decision making: *keeping up with the Joneses*. It is an approach that security technology vendors adore, because they have a variety of ways to claim that other firms use their tools and techniques. It is this approach that led the firm in the previous example to deploy the useless detection technology.

In my tenure as a security officer, if I were to believe all security salespeople, I would never have seen a security product that Citi does not use. Vendors knew that Citi was so huge that no matter whom I called there, the person could never be sure that there was not some department somewhere in the company using the software. Occasionally, I would also hear a claim from a salesperson that some other department at Bear Stearns was using a given product. As we were a much smaller firm with centrally managed global infrastructure, I knew it was impossible for anyone at Bear to be using a security product that I did not know about. Yet even when I told vendors they were wrong, they never admitted to lying. They would either say that they could not remember the name of the person with whom they supposedly were doing business, or they would backtrack and say they had made progress in a proposal to someone in another department, and it was their belief that he or she was in a position to evaluate the product for use at Bear.

Both the cost/benefit approach and the *keeping-up-with-the-Joneses* best-practice approach to security decisions are based on an underlying assumption that security can be achieved through a series of projects. On the opposite end of the security management spectrum is a holistic view of security, in which security management systemically aligns with business

strategy. Security managers generally agree that those who implement systemic Security Programs have more control over assets and operations than those who do not.<sup>6</sup> Though there is not a lot of hard data, stories of how systemic Security Programs directly bolster a company's ability to conserve assets and maintain control under change are emerging.<sup>7</sup> There is also an academic study showing that firms with IT material weaknesses in their financial reporting system are associated with higher likelihood of turnover of both IT and non-IT executives.<sup>8</sup> Because IT material weaknesses are generally related to poor information security, this study provides anecdotal evidence that poor security is correlated with systemic management weaknesses.

Furthermore, despite the bad press that security horror stories get when they motivate bad solutions, there are many true security horror stories that illustrate the fact that, in the absence of systemic security management, disasters do happen. So, for purposes of illustration, this book will sometimes cite a real and true security horror story (SHS). These illustrations will always be based on factual cases, never exaggerated to make a point. Descriptions of non-public incidents may be vague to minimize the possibility of revealing the company's identity. Descriptions of publicized incidents may be accompanied by citations. An SHS will not be used within the text as persuasion, but will be clearly demarcated as an illustrative example. It will be numbered for easy reference, and offset from the rest of the text. For example:

### **SHS1:**

---

During sensitive legal negotiations, a company's lawyers discover that the counterparty seems to have ongoing access to inside information that has been shared only with the highest levels of management. An examination of the email system reveals logs showing that the CXO mailed sensitive information to an email address at Yahoo. Yahoo will not provide any information as to the owner of the recipient's email box. Consultants are called in. They investigate and find that another employee communicated with the same address at Yahoo several months ago. That employee is interviewed and confesses that he logged into the CXO's mailbox and sent himself copies of the CXO mail, which he shared with the legal counterparty. When asked how he knew the password to the CXO mailbox, he divulged that all passwords in the company were the same as the user's last name.

This example illustrates that one person's SHS is not necessarily a source of FUD for another. For a security professional, this SHS describes a routine and minor security incident. Routine, because so many companies allow users to have easy passwords because then they never have to bother to reset them. Minor, because the root cause of the SHS is easy to solve. This SHS has well-defined solutions that are easy to implement.<sup>9</sup>

For a security professional, an SHS should be a tale of things that happen to others. SHSs are by definition preventable. What puts the word “horror” in the term *security horror story* for security professionals is not so much the bad consequences, which can happen to anybody, but the absolute embarrassment involved in admitting to not having established systemic security aligned with organizational requirements. Good security professionals know that these things should not happen on their watch. They do everything they can to avoid security horror stories. Unfortunately, they often do not have the management acumen and/or support required to accomplish their career goals.

Though CXOs are not expected to take responsibility for day-to-day security practices within their firms, there are things CXOs can do to make sure security horror stories don't happen on their watch. Staying above the threshold of obvious vulnerability through a systemic security posture does require CXO commitment. Systemic Security Programs of course include the use of professionals who recognize when off-the-shelf solutions for security problems are well-known. Where systemic security is well done, a security horror story should not result. For a CXO, security responsibility is not at the implementation level, but at the security strategy level. It is precisely in the situation where no obvious solution is available that the choice of an appropriate solution requires CXO involvement at the strategy level.

So, rather than wait to be pulled into security decisions just when money is required on some project whose justification is based on some guesswork, I advise CXOs to promote a security strategy and policy that is easily understood and flexibly implemented. Once a base level of security is firmly established from the top down and integrated with organizational strategy as a whole, it is easy to add controls that make sense to the organization as a whole, and less easy for any one department to claim unrealistic potential from a project that does not align with the organizational strategy.

This book is about how to accomplish security through tone at the top.<sup>10</sup> It is not about how to accomplish security measures, but how to cultivate a culture that preserves organizational assets. Careful planning in security strategy lessens the likelihood that incidents will occur. Certainly it will help prevent security horror stories from happening on your watch.

*This page intentionally left blank*

## CHAPTER 1

# TONE AT THE TOP

Tone at the top exists whether you set it or not. It is reflected in how you lead to ensure that people think about the things you really care about. For example, it was widely known within Bear Stearns that the CEO, Ace Greenberg, had grown up knocking on doors and making cold calls. He had a good pitch, but he had trouble getting people to listen to it. So one of the things that mattered to him was how his employees reacted to cold calls. Whenever he heard about an employee ignoring a solicitation call, he would call the individual personally, verify the facts of the case, and berate the individual for inappropriate and unprofessional behavior. It was OK to turn down unwanted solicitation, but you had to give a new pitch a chance. Years after Ace retired as CEO, though he was still on the board, a colleague of mine at Bear was targeted by a vendor and neglected to return several cold calls over a few-week time period. She got a call from Ace. It took more than three rings for her to answer it. Not only did she never neglect to return a phone call again, she told the story of being berated so emotionally that no one in her circle of work acquaintances ever did either.

There is no single right way for a CXO to make sure people really understand and internalize the things that are important. Not everyone is as direct as Ace. But consciously or unconsciously, every good leader has a method of getting important messages across. Many CXOs make it a practice to always be at the same level of calm so that they get maximum value out of showing emotion with respect to an important issue. Others

work at a brisk pace, but slow down when explaining something they think is really important. Some never seem perturbed at all, but occasionally unexpectedly fire someone who seemed to be competent, but was perhaps passively resistant to the CXO's vision. Management books may abound with advice on how to get people to do what you want them to do, but no amount of behavior training will result in the completely consistent behavior toward an issue that is produced by actually caring about it.

## LEAD BY EXAMPLE

The usual evidence an employee will have on whether a CXO cares about security is whether or not the CXO follows security procedures. After all, a CXO is usually very far removed from those who create security procedures. It is very easy to observe whether a CXO follows security procedures or not. If the perception is that the CXO does not follow security procedures, then no one will believe that they will actually be held accountable for violating security procedures either. Indeed, if there is a culture of negligence when it comes to violations of security procedures, then employees can convincingly claim that no one is accountable for following them.

Where a CXO does not follow security procedures, it is usually because the procedures do not make sense to the CXO. If procedures don't seem to make sense, the CXO should be concerned about lack of productivity resulting from the fact that people are following them. If the procedures don't make sense, they are probably are not much help in protecting assets either.

A CXO who does not follow security procedures probably also does not consciously connect concern over assets with day-to-day security procedures. Concern over assets reflects a distinct view of the organization. That view is based on current and future value of the people, processes, facilities, inventory, and technology that are required to execute tactical and strategic business plans. It includes current physical plant, human resources, communications channels, and financing. It also includes the current state of future planning for such things as new locations, technology, Internet presence, and retail space.

The trick in setting a tone at the top that supports asset preservation is to have security that makes sense. It is important to keep in mind that *tone at the top* exists with respect to security *whether or not* a shared vision of assets is cultivated. Even if there is not a real attempt to communicate on security issues, there will nevertheless be a message that reaches the staff. If the message is that security is not important, that could have bad consequences for assets. Consider the following security horror story.

**SHS2:**

---

The entrance protection at an office building in a large metropolis includes a reception desk and a physical security guard standing by an elevator 20 paces away. Employees show badges to the guard prior to getting on the elevator. If the guard sees that a person does not display a badge, that person is sent to the reception desk. The receptionist requires the visitor to state what company is the recipient of the visit, present identification, sign in, and wait while the receptionist calls upstairs to ask the company for approval to send the visitor back to the elevator. The guard is to observe this practice and let the visitor through only upon completing the receptionist sign-in procedure. At this building, several major objects of value disappeared. No one saw anything. No visitors were signed in that day. Acknowledging that security was inadequate, management installed badge-activated doors and cameras in all the office spaces. The next incident of theft came a year or so later. However, no one could pinpoint when the theft had occurred. It was sometime over a two-week period between the last time the object was directly observed and the time it was discovered to be missing. The administrator of the badge and camera system was tasked with finding the culprit. The system had been installed by a vendor, and the administrator had never actually run a report before. When she tried to run it, the system crashed due to inadequate memory, partly because the logs for the past year had been straining the storage resources on the system. The data was unrecoverable. When she tried to play back the camera system, she found that it stored only a week's worth of images, and it had no viewable fast forward feature, so to review a week's worth of images would have taken her an entire week's worth of time. They gave up on investigating the incident and started looking for a new camera system.

The guard and receptionist procedure may seem like security to the average visitor, but there are many ways to defeat such a system. Someone could wait until the guard was not watching and sneak in. Someone could purposely divert the guard by asking for assistance with a large package while an accomplice got onto the elevator. Someone could sign in at the reception area, then tell the receptionist they are in the wrong building, walk a few paces toward the door, then turn back toward the guard post as soon as the receptionist becomes engaged with the next visitor. In the environment that

led to SHS2, it was also common for visitors to walk in accompanied by employees. The CXOs even nodded and smiled to the guards as they escorted visitors in without seeing the receptionist.

The badge entry and camera system looked like good security, too. But, in the SHS2 environment, it was common for visitors to follow employees into the elevator even if they did not know them, counting on the fact that it was also common for badge-holders to open doors for visitors in the office spaces, whether they recognized them or not. Even if the camera system had worked, the assets were already gone by the time the thief could be identified. If it was not an easily recognized individual, it would provide little evidence by which to retrieve the asset, especially if he or she was disguised. Even if the individual was identified, the asset may not be found.

In the security profession, the phrase used to describe the type of security in SHS2 is *keeping your friends out*. Or, as one prominent security professional puts it, “Security Theatre.”<sup>1</sup> The security is there so that those who observe it will feel that security does exist there, but people can easily get around it because there is no actual control in place. In SHS2, the company was paying for security supposedly to have some measure of control over who gets into the building, and to identify who was there. That security did not work. The company did not plan any controls over which objects could be removed from inside and carried out of the building. So the security did not accomplish the goal of reducing theft. It inconvenienced the honest visitor for no added security benefit. It required the employee to carry a badge around while not preventing the non-employee from getting in. It required a system administrator to issue badges and install a camera recording server but could not produce evidence of who was in the office. One may argue that criminals may be deterred by having to make a plan to get around the guard, or that they would have to know someone in the company to be able to follow them in without fear of getting caught. But everyone understands that there are better ways to deter potential criminals with the same or less degree of inconvenience for friends.

Note the word “everyone.” It is not just security professionals who recognize ineffective security activity when they see it; it is every thinking person who decides to analyze it. If an employee in the scenario of SHS2 actually observes an unauthorized person coming into the building, he or she does not report it. The place to report would seem to be the same security people who are practicing the bad security. But, because employees know the CXO walks through the same doors that they do every day, they assume that the level of security that allows unauthorized access is accepted by the CXO. They have observed entranceways in other buildings where the guard at the elevator requires visitors to have a pass issued



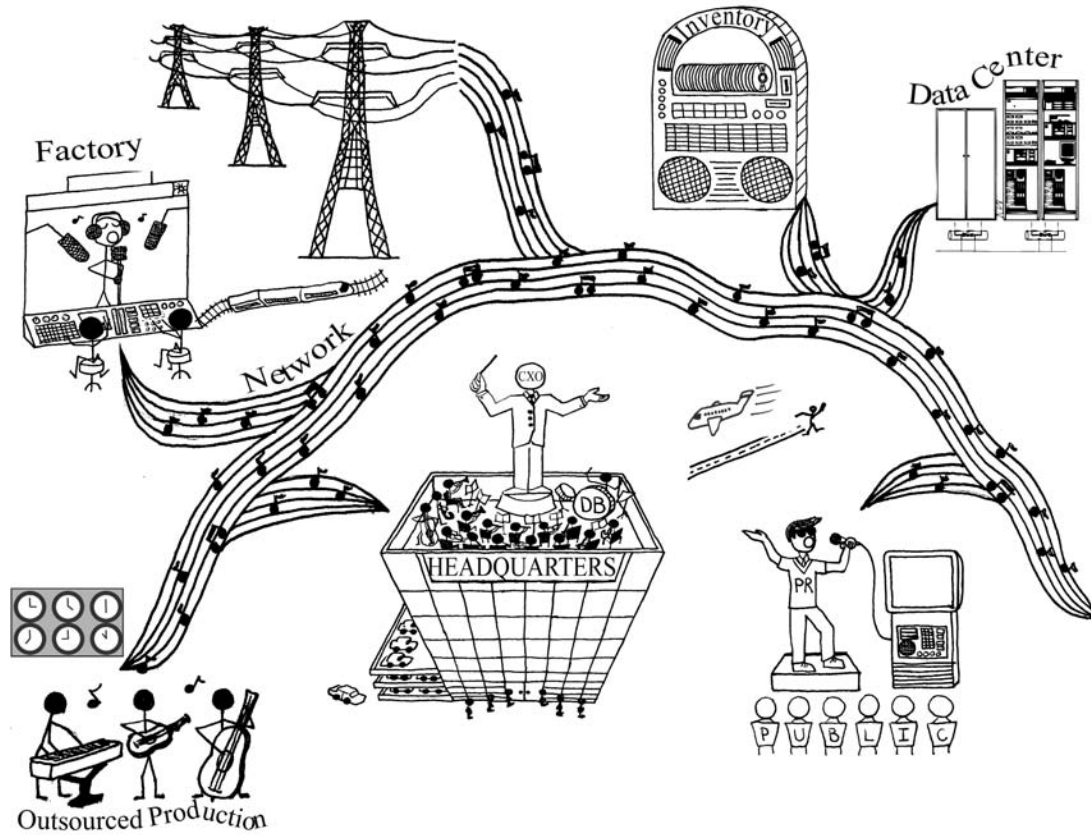


Figure 1-1: Example of Asset Landscape

by the receptionist. They have seen badge-activated turnstiles in other buildings. They know it would be easy to improve procedures, and the CXO does not bother, so why should they?

Of course, I am not suggesting that the CXO should have to pay attention to every last management detail with respect to security. But there has to be some coordination at the CXO level to ensure that someone is taking care of an overall strategy for covering the asset landscape. *Fire and forget* may work as a management strategy with top sales executives, but it is not likely to empower security personnel to accomplish organizational goals for control over assets. Moreover, most security professionals do not have a good understanding of the asset landscape of their organization, so they fall back on procedures they learned at their last job, or those that come with the building or computer system. It is unlikely that this fallback behavior will be optimal, or even satisfactory, in every situation to which it is applied.

A CXO should recognize that few security professionals will ever be able to envision a CXO's asset landscape nearly as well as the CXO. They can only approximate it with models such as that in Figure 1-1. It is up to the CXO to help them build a mental model of the asset landscape that includes everything of significance to the CXO's vision for the company's future.

## SUPPORT THE TROOPS

Even where the security professional understands the asset landscape, and is directly following CXO vision, the CXO should also recognize that an important security objective may seem to be at odds with other CXO objectives. In the SHS2 scenario, the CXO may want to be able to escort clients into the building unimpeded. A security objective to identify all visitors may seem to require exceptions. The risk in such exceptions is evident upon review of situations like the one in SHS3.

### **SHS3:**

---

“A New York City councilman was killed inside City Hall yesterday afternoon by a political opponent who accompanied him to a Council meeting, pulled out a pistol and shot him in front of scores of stunned lawmakers and onlookers, officials said. . . . [The gunman] was apparently able to slip his gun into City Hall by accompanying the councilman, who did not have to pass through metal detectors, officials said. . . . The shooting occurred at one of the most heavily

protected sites in the city. While Mayor Michael R. Bloomberg has been credited with making City Hall more open and accessible to the public, all visitors are required to pass through airport-style metal detectors before entering, except for elected officials. . . . The shooting led Mayor Bloomberg to declare that from now on everyone, including elected officials, would have to pass through the metal detectors.”<sup>2</sup>

In SHS3, the councilmen were privileged with an exemption from security rules until Mayor Bloomberg decided no more guns were getting into City Hall under his watch. It is not uncommon for management directives to have unintended consequences for security. If a CXO message to the minions is that sales always comes first, security may be sacrificed when salespeople make presents of company laptops to friends and family. If a CXO message to the minions is that productivity come first, a manager may be hesitant to challenge the desktop technician who claims to need access to everyone else’s login password in order to assist them as quickly as possible. Security procedures that are just common sense to security professionals should provide a sanity check against unintended consequences with respect to security.

Unfortunately, the burden is currently on security professionals to join management ranks in order to ensure that commonsense procedures prevail. Since the 1980s, they have been urged to “relate to senior management goals and must be considered part of the management process.”<sup>3</sup> This tack is not working. They are being urged by their professional associations to fully understand the business and excel in Dale Carnegie training programs. Alternatively, tone at the top can provide support for the commonsense asset preservation procedures that are the security professional’s field of core competency.

A tone at the top that emphasizes control over assets can cultivate a culture at the minion level that respects thoughtfully selected security measures. The more people in your organization who understand the importance of those assets, and the way security measures work to preserve them, the easier it will be for an individual security guard or administrator to stare down a high-profile adversary. They will find strength in the CXO message that protecting assets from fraud, crime, and neglect is an important objective; this resolve, as with any successful management strategy, begins with tone at the top.

Without deliberate effort, CXO tone at the top with respect to security will be a conglomeration of perceptions that get created by the security guard at the front desk, the help desk responsible for resetting passwords, and the application screens that people sit in front of every day. If there are visual cues that security personnel are slacking off, and these cues clash with sincere and emphatic CXO directives to preserve assets, then conscientious staff will comment, complain, and eventually escalate. But if there is no clear message with respect to security, the slackness will be perceived as just the way management feels about security, and the staff will assume that accountability for security measures is not routinely enforced. They will be similarly security-slack in their own day-to-day endeavors. In few other fields does the adage “if you are not part of the solution, you are part of the problem” apply so well.

People can also tell what a CXO cares about by level of personal involvement. Of course, a busy CXO cannot be all things to all people, but it does pay to be familiar with where the security function reports, and to ensure that it is supported by an internal champion who has access to a CXO’s ear. If the security department is hovering under the Compliance Department, Building Services, or the Office of the Comptroller, it probably looks to your management team like a necessary cost center as opposed to an instrument of management. Placement under a Chief Operations Officer (COO) or, in the case of Information Security, a Chief Information Officer (CIO), would instead place it in line with the strategic objectives of the business. It encourages security goals and objectives to be integrated with daily decision making with respect to the assets under the corresponding department’s management.

There is an argument that security cannot be placed under the management of the department that operates the assets to be secured because security costs money. The argument is that the management will want to lower its operating budget, so will be happy to hide security deficiencies, because this will save money that might be spent fixing them. For example, they argue that a CIO will not require administrators to securely configure machines because it costs money to do so. I have always found this argument absurd. The CIO is the first person to want those machines to be securely configured. If the machines are not secured, data integrity could be damaged accidentally or intentionally by an unauthorized user, with the result that the CIO will not be certain that the machines will continue to operate properly. That is, the incremental amount of time and effort it takes to correctly secure a machine as opposed to leaving it unsecured pays back in operational reliability and incident recovery. Any CIO who

does not know this will fail for reasons other than not properly supporting security objectives. The only argument for segregating security-related duties from the management of assets they are designed to protect is to provide oversight akin to audit of the management function.

Such purposeful segregation, sad to say, often results in an *artificial* tone at the top. In organizations with a security culture deficit, tone at the top with respect to security is sometimes deliberately and artificially created by a security officer in order to pass an audit. A mission statement so uncontroversial as to be trivial is presented to the CXO, who signs on the dotted line below it. It is posted on the organization's internal network, and it may also be distributed in memo format. In well-funded departments with regulatory compliance obligations for security measures, the CXO may even be persuaded to read the statement into a video camera, and that message may be required viewing for employees in certain job functions. That action meets regulatory requirements for tone at the top, thus providing true significance to the phrase *good enough for government work*.

An artificial tone at the top is created by a security professional for the simple reason that, without the endorsement by leadership in a recognizable form, the security mission statement carries no weight with regulators. Auditors understand that people are not accountable for doing anything other than what is in their job function. So if job descriptions do not include security, the easiest way to work in some accountability is with an executive directive. The artificial tone at the top creates a paper trail that allows a CXO to claim that responsibility for security is assigned (even when, in fact, it is not).

Another observation on the artificial tone at the top is that, though the visible endorsement method makes tone at the top easy to demonstrate, and is good enough for government work, it is easy to see through. If there is no indication that security is taken seriously elsewhere in the organization, and especially if there are observations of the keeping-your-friends-out method, then there will be no expectation on the part of the staff that their behavior should be modified in order to comply with the security mission statement. In the same way that torn furniture fabric and worn carpet send signals that management has no pride in appearances, poor security communicates that management has no pride in protecting its value. The truth is that this approach will not even work on auditors. If they see evidence that assets are not adequately protected, auditors will not believe that the security mission statement is any different from any other regulatory filing. They will doubt the integrity of the CXO's statement to the video camera, and everything else the CXO says as well.

Water-cooler talk about bad security is no different from talk about any other aspect of a dysfunctional organization. Once people start finding fault in management, they quickly start extrapolating and criticizing all kinds of organizational handling of things. This easy ridicule brings down morale and fosters disrespect for a wide variety of associated management processes designed to protect and preserve value. Why keep inventory if the laptops just walk out the door anyway? Why use unique logins when everyone has the same password? Why sign for petty cash when no one reconciles it anyway?

## STRATEGIC SECURITY

Whether or not there is professional security management and common-sense practice within an organization, a CXO can still foster a healthy respect for business value. It could be real estate, physical plant, technology, people, or even process. Estimation of value should not be confined to assets that can be bought or sold. Operations workflow is often a huge source of value. The asset landscape should include everything that it is worth devoting energy and effort into securing. In developing an asset landscape, use the Latin phrase “*sine qua non*” as a guide: “without which, nothing.” Which people, processes, objects, or intangible traits, such as reputation, are so important that, were harm to come to them, immediate harm to business would result? What is the *sine qua non* of the business? This is how to start thinking about security. Security should be designed to preserve value.

A tangible vision of an asset landscape does not have to be a picture. It can be a list. It can have unknowns or delegated components. For a CXO, the aim in producing this vision is to be able to verify that, if the security management team was to sketch their version of the landscape, would that drawing or list be remotely the same? What would be the areas of highest overlap? The lowest? Now, how can a CXO make it known, beyond a shadow of a doubt, that anyone who fails to properly secure that asset landscape is actively working against the current and five-year business plan? How many of those things of value consist of information that needs to be kept confidential in order for plans to really take root? How many rely on accurate information gathering and processing? How many must simply be available in order for plans to be completed? How many must be acquired, and are there controlled processes in place to accomplish the acquisition? This is the basis for a *Security Program*. A Security Program is the organizational framework whereby assets are catalogued and due diligence measures are taken to preserve their value.

Security measures like the ones in SHS2 often look silly to people because they are delivered without consideration of exactly what they are designed to protect, and without a comprehensive view of how the security measures contribute to asset protection, a view that a Security Program provides. Whether or not there are security guards at the doors of your building should be one outcome of an asset landscape protection requirements analysis. The plan in SHS2 failed because it was not focused on the assets themselves. Strategy for protecting objects normally includes safes or container locks, alarms, tracking devices, and bag searches (to name a few). Instead, the security mechanisms put in place were focused on the people going into and out of the building. There may be other assets that would benefit from those security mechanisms, but not the ones that were the target of the exercise.

Deciding how to secure an asset is not an easy task. For example, suppose one of your prized assets is product inventory. Your security strategy may be to keep it all in a factory warehouse until there is a bona fide purchase order indicating it should be shipped to a customer. Implementation of this security strategy requires not only physical security measures, but may also require a complex interface between a customer order management system and a warehouse automation system.

Like any management strategy, managing security has a continuous feedback loop that allows for mistakes in implementation to be recognized and corrected. Once it is clear why security may even be necessary, there must be some high-level management agreement on how it may best be accomplished. Some person or committee has got to look at the asset landscape and figure out what mandates should be in place in order to protect it. These could be as simple as these:

- “All data used to run the physical plant should never leave the plant unless through a process controlled by information technology, and then, only for the purpose of archiving recovery data.”
- “All information concerning our customers will not be shared with anyone who does not have an immediate need to know to accomplish a service or task on the customer’s behalf.”
- “All product inventory will be stored only in company warehouses unless it is in the process of being shipped under a customer purchase order.”

These statements are examples of security policy. It may not be immediately recognizable because security policy is often based on some arcane government standard that is generically known to be of use in creating a

Security Program.<sup>4</sup> But these statements are the only type of security policy that will have the same significance to a CXO and the staff. They should be phrased as mandates that have no exceptions.

Once some set of statements is formulated that distill the security strategy into comprehensible policy, the next step in a security management cycle is to make sure the staff is aware of them. This awareness activity may look like the same video statement written by a security person and spoken by a top executive that was previously denigrated as an artificial tone-at-the-top approach. But if it actually has the CXO asset landscape and CXO-endorsed mandates as its core, it will actually be genuine tone at the top. When policy is definitively decided, a CXO simply needs to make people aware of those decisions.

Effective security awareness is often supplemented with memos, posters, and formal training programs. But in order for it to be consistent with tone at the top, it should not deviate from any other important directive the CXO has issued on any other topic. If posters are not ordered when providing important direction on a strategic business process, they should not be used to promote security. Superfluous and out-of-character measures are always seen as products of the security staff rather than of the CXO.

Once the CXO message on security has trickled down, each manager who has any control over the process for handling assets should be executing according to the policy, or jumping up and down saying why he or she cannot. If it does turn out to be impossible to comply with policy, policy should be immediately changed and strategy revisited.

A CXO's first foray into setting tone at the top for security often encounters a "risk manager." Because of the plethora of "industry standard" but impracticable policies in the security literature, there is often a case made to allow some subordinate to decide that he or she can "accept the risk" of not being security-policy compliant. This is equivalent to a policy exception. Policy should be flexible enough to be implemented without exceptions, or it should be changed. A comptroller would not let subordinates change accounting policy without escalation, and potential rewrite of accounting policy. A human resources manager would not let subordinates decide when to enforce a sexual harassment policy. Likewise, there should be no reason for a CXO to allow exceptions to a policy designed to protect the asset landscape. Where the CXO policy is not forced by some external regulator or from some internal well-meaning but dysfunctional security department, it will be exactly what the CXO has decided needs to happen to preserve assets. Allowing even one circumvention fosters disrespect. Policy should instead be designed to allow flexibility in decision making without bending on critical aspects of securing assets, and it should be changed when necessary.



Another behavior that will foster disrespect for policy is complacency. A policy that is never monitored becomes disposable quickly. Where there is no consequence of non-compliance, people will naturally make decisions based on other criteria such as expediency or cost. This may fulfill other goals a CXO has set that are being monitored, such as product delivery and budget. Where there is a trade-off, what is measured will be met at the expense of things that are not measured. Compliance with mandates must be measurable.

Note that those who implement security may have issues demonstrating compliance. Though these demonstrations need not be part of policy, they may nevertheless be dictated as a “policy implementation standard.” This puts pressure on those implementing to make their compliance transparent without raising the compliance monitoring process to the policy level. However, the compliance method may be more flexible than the policy itself, and this may sometimes allow for creativity in the demonstration. Unless measurement processes qualify as security mandates at the policy level, allowing alternative approaches demonstrates flexibility and reinforces that the tone at the top is reserved for the strategic objectives itself, rather than for any given procedure.

Invariably, the monitoring process will yield cases, perhaps inadvertently, of policy non-compliance. These may be simple to remediate or may actually be so problematic that they cause a change in strategy and also perhaps a change in policy. The feedback from the remediation activity into the security management process completes the security management cycle’s continuous feedback loop.

Figure 1-2 illustrates that security requires a continuous improvement process as much as any other aspect of management. Security management models have been called *Plan-Do-Check-Correct*, *Plan-Secure-Confirm-Remediate*, *Prepare-Detect-Respond-Improve*, and *Restrict-Run-Recover*.<sup>5</sup> All of these security management models follow a management model recommended by Deming,<sup>6</sup> It is one with which the vast majority of CXOs are extremely familiar, namely:

- Have a plan
- Act according to the plan
- Make observations in order to see the plan is working
- Make changes to the plan based on the observations

Where Security Programs are based on management objectives, the security management model also follows the recommendations of Drucker, to manage by objectives and self-control.<sup>7</sup>

While a CXO will likely not be managing security at the level of the feedback loop, whatever loop is used within the organization should be

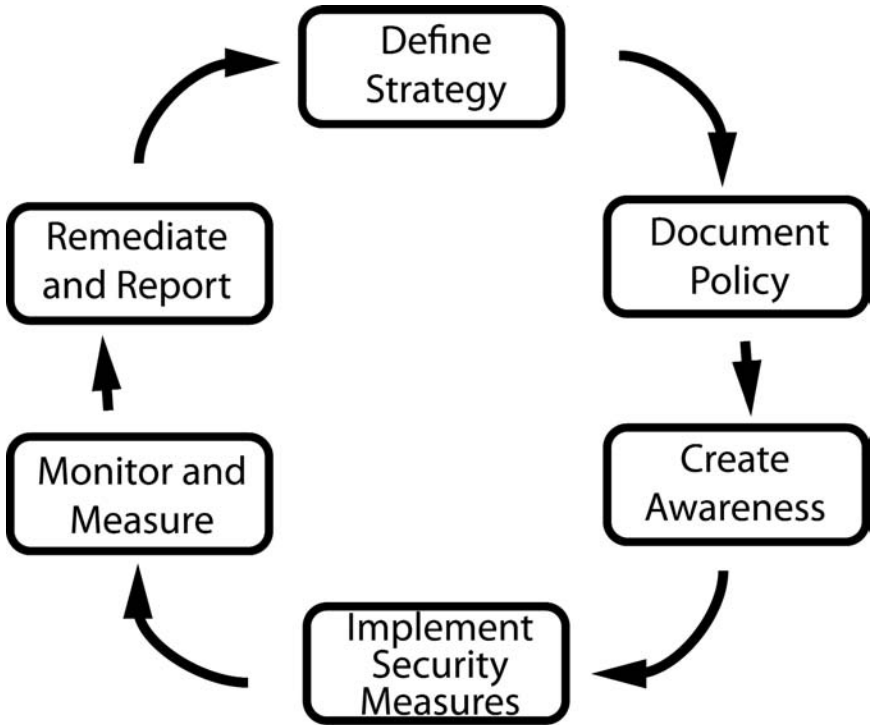


Figure 1-2: Security Management Cycle. Adapted from Bayuk, Jennifer, *Stepping through the Security Program*, ISACA, 2007.

well understood by the CXO, and it should have enough touchpoints with CXO management style to enable the CXO to influence the overall program. These touchpoints should be visible to both security personnel and the rest of the staff. Careful selection of CXO touchpoints within security management process allows a CXO to influence security without overseeing its daily operation. The remaining chapters enable a CXO to recognize and/or create touchpoints effectively in order to efficiently provide tone at the top for security management.

## CHAPTER 2

# THREATS AND VULNERABILITIES

Security professionals often use analogies to make a point. I almost hate to repeat the joke about the bear because it is so overused. But the fact that it is so often used in the security profession means that this book would be incomplete without it (Figure 2-1). So here is the joke about the bear:

Two friends are out backpacking and inadvertently get between a bear and her cub. They can tell that the mother is getting ready to charge. One of the friends takes his sneakers out of his backpack. Throwing off his hiking boots, he puts the sneakers on as fast as he can. The other friend yells at him to get moving, “Why are you delaying?” he says, “You will never be able to outrun a bear!” The friend with the sneakers says, “I don’t have to outrun the bear, I just have to outrun you!”

The analogy with this joke and security measures is that criminals prey on the weak and vulnerable. Given the choice between two office buildings, one with only a cylindrical lockset and the other with deadbolt locks, they will break into the one with the cylindrical lockset because doing so is easier. Given the choice between two Internet sites, one that restricts administrators to an internal network and one that allows administrators to make changes to the site from the Internet, they will attack the latter because that is easier.



Figure 2-1: The Bear Analogy

## THE PERIMETER-ATTACKER VIEW

In both physical and logical security scenarios, there is a concept of a perimeter. The perimeter is the external boundary of the area that an organization attempts to restrict to specifically authorized purposes. Where there is no attempt to restrict access, no perimeter has been created. In physical space, the property line serves as a good first draft of the perimeter. Nevertheless, a security organization may decide to put their fences a few hundred yards closer to the building than the property line. A residential security perimeter is often the front door. The analogy with cyberspace is the marketing web server. Users clicking around your marketing Web site are as expected as pedestrians on the porch outside your building. They are within your space, but external to your security perimeter. There is no attempt to restrict that type of access.

In addition to security measures that restrict, there are security mechanisms that monitor. These may go beyond the perimeter and even beyond the borders of the organization. A camera may record images from the public street and nearby buildings. A scanner may comb the Internet for a proprietary logo on other people's public sites. Monitoring security measures do not prevent attempts to penetrate the perimeter, but they do deter attacks if attackers can tell they are there. The bear analogy dictates that security professionals should be looking at their neighbors and competitors to see what restrictions and obvious monitoring they have in place, and go just one better. The lesson of the bear analogy is that, if you have more restrictions and more obvious monitoring than the organization next door, the attackers will go after them instead of you. SHS4 and SHS5 provide good examples in the cyber and physical security arenas, respectively.

**SHS4:**

---

“Prosecutors allege that [defendants] first hacked into a wireless computer system at an unidentified BJ’s Wholesale Club store around 2003 and stole customer credit-card data. In 2004, [defendant] allegedly gained access to debit-card data at an OfficeMax store in Miami. . . .

With access to the server, the defendants installed ‘sniffer programs’ that captured payment card data as customers were making purchases throughout the retailer’s stores, the indictments state. Using their own direct connection to TJX’s computer system, they repeatedly downloaded the data, which they sold or used to create their own credit cards, prosecutors allege.

TJX didn’t discover the breach until December 2006 and didn’t announce it publicly until the next month.”<sup>1</sup>

**SHS5:**

---

“Police say thieves targeted an unmanned building owned by telecoms giant Cable & Wireless at around 3:10 am this morning. . . The company, which confirmed its office in Ryan Way suffered a break in, has not confirmed what was stolen. It is believed, however, that optical wiring, computers, routers, servers and switches were removed from the site. . .

The theft has been blamed for knocking a number of high-profile sites off-line, including Sainsbury’s, Ordnance Survey and the Financial Times.”<sup>2</sup>

The TJX story was a wake-up call for all who thought that they did not need to protect wireless traffic. The Watford data center story was a wake-up call for anyone who thought it was OK to consolidate monitoring of multiple buildings in places far away from most of them. Strong encryption of wireless traffic and onsite security guards were the sneakers of the day. This is why the bear analogy is so often repeated.

However, the bear analogy does not present the complete picture. It assumes that the attacker is external to the victim. This leads security

professionals to assume that organizations always have a perimeter, and that there is an attacker who makes a decision with respect to penetrating that perimeter. The perimeter-attacker view of security has created some complacency with the level of security in many organizations, both physical and cyber. Some vulnerabilities, though, just don't need attackers to be exploited: there are plain weaknesses inside the perimeter of the organization that threaten assets. These internal vulnerabilities can be self-defeating. Weak ceilings and fire hazards can reduce building value and destroy inventory without one intentional act of harm. The same point is often made about cyberspace. One book that does a great job putting cyber security issues into layman's terms asks the reader to envision a bridge that has the following engineering and safety problems:<sup>3</sup>

- The steel, cabling, and concrete used to construct the bridge are riddled with structural flaws.
- Engineers have concluded that the bridge could fall down if these flawed components are not patched quickly.
- The surface of the bridge is seriously impaired and the required refinishing sometimes weakens the overall structure.
- Bridge operators utilize a notification system that provides real-time information about any bridges that might be falling down.

A CXO who knew about that bridge would be criminally negligent not to fix it. But many companies routinely run on vulnerable software every

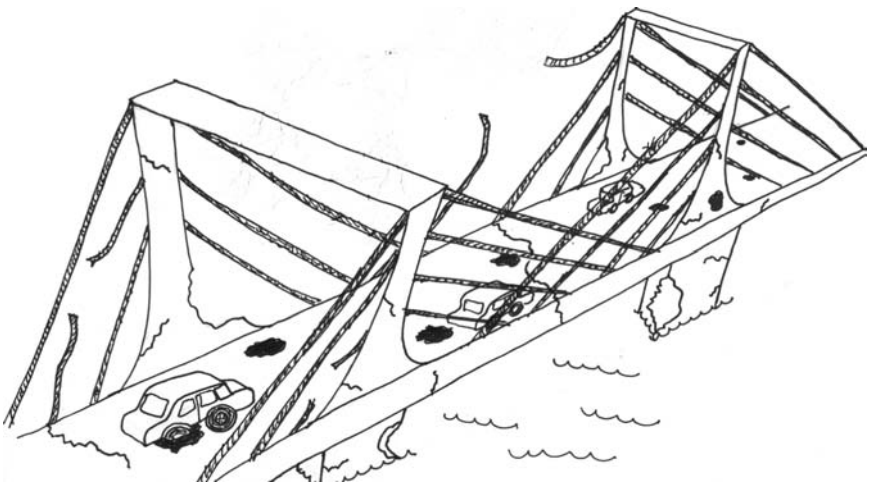


Figure 2-2: The Bridge Analogy

day. The “notification” system is analogous to a security monitoring measure that will alert them when it finally falls.

The key word in the software architecture to civil engineering analogy is “patch.” Everyone knows civil infrastructure needs to be patched occasionally to remain resilient. In computer science, this type of fix is also called a patch. The word *patch* in a computer context comes from the days when computers were programmed with cables plugged into electronic circuits the size of walls. Patches were the cables that altered the course of electronic processing by physically changing the path of code execution. Computer patches are now bits of software that replace the faulty ones. Due to a wide variety of constantly changing technical glitches, patches have to be downloaded from the software maker all the time in order to keep the software working properly. They are not just issued to fix vulnerabilities that are exploited by criminals. Most patches are intended to protect against vulnerabilities that make systems malfunction without being attacked at all, such as leaky memory and structural design flaws.

## THREAT LANDSCAPE

Another complexity that destroys the bear analogy is the known fact that most crimes against information assets are done by people who have once worked, or still work, within the organization that is the victim. This is colloquially called the insider threat. Given the sum total of people who have the ability to destroy information assets, the ratio of those that are outside the perimeter compared to those inside is very small. Those already inside can do more damage more quickly, and usually without detection. Using actual case data provided by law enforcement, researchers at Carnegie Mellon University analyzed 190 cases of verified insider cyber crimes. These are summarized as SHS6.

### **SHS6:**

---

Of the cases studied by Carnegie Mellon, about 40 percent involved IT sabotage against their employers’ systems, about 40 percent were classified as theft for financial gain, and the remaining were either for competitive advantage or miscellaneous reasons. Those that committed sabotage were mostly disgruntled or recently discharged high-level technical employees who retained access via system administrative and other shared computer accounts. Those who stole for financial gain were usually low-level employees using

authorized access to engage in fraud, collaborating with outsiders in two-thirds of those cases. Those who stole for business advantage were almost exclusively employees leaving the company to go to a competitor. Virtually none of these cases were detected by security personnel. The sabotage was mostly detected through operational failures. The fraud was commonly detected by the finance department, or tips from suspicious individuals both inside and outside the organization. The business advantage cases were usually detected by customers, law enforcement, or the sudden emergence of a qualified competitor.<sup>4</sup>

What is most interesting about the Carnegie Mellon study is that it provides information only about the insiders who were caught. Excluding the cases that resulted in sabotage, the majority of the cases were not detected by the organization without assistance from outsiders. This situation indicates that the insider threat is always likely to be larger than it appears to anyone in security.

Nevertheless, the bear analogy worked well for security personnel in the early days of the Internet. For a long time, Internet hackers<sup>5</sup> were randomly looking for vulnerabilities that could be exploited for gain. They did not always know how they could make money by hacking a particular target; they were mostly lured by vulnerabilities. Once they broke into a system, they would figure out if they could exploit it. They would find information and then query the black market to see if someone would pay for it. The bear joke analogy made sense because, although the threats were ubiquitous, if your security was a little better than the company's next door, then the hacker would likely break into its system instead.

But now, even assuming no internal threats, integrity in patching, and a well-defined network perimeter, Internet threats have changed the cyber threat landscape. Anyone connected to the Internet will eventually be targeted, and many otherwise honest individuals are often guilty of aiding and abetting through negligence in security controls. Keeping one step ahead of standard protection strategies may no longer work.

The last time I heard the bear joke at a security conference, the ending had changed. The speaker, an expert in global cyber security investigations, said, "You used to only have to outrun your friend, not the bear. But, bears either eat, sleep, or make more bears—unless you and your friend



work together to fight the bears, eventually there will be more bears than friends and you will all be eaten.”<sup>6</sup> The likelihood of being a target now has nothing to do with your defenses. A new popular analogy in security circles is that *you don't have to be a target to get shot*. It is as if the Internet community is a crowd into which someone is randomly firing a machine gun. The Internet has leveled the threat landscape to the point where everyone is susceptible to widely distributed attacks. This is not meant to generate FUD. It is just a simple statement of fact.

Organized crime has always been a subject of management attention in the transportation and manufacturing industries. In the dawn of the computer age, it became a factor in the telecommunications industry because criminals figured out how to defeat computer-controlled phone systems and get free service. Now, organized theft of service can actually seem to be random. SHS7 illustrates the point. It is a multi-step scam, and may be better understood with reference to Figure 2-3.

### **SHS7:**

---

An organized crime unit operating out of Russia devised a program that runs on a computer and intercepts all the information that the computer user types into any Web site and sends the information back to a site in Russia. The same group broke into several vulnerable Web sites frequented by U.S. consumers and altered those Web sites so that when a user clicked on certain links, the Web site would download the interceptor program and install it on the user's computer. The Russian group then established its own Web site to sell bank account and credit card company login information to other criminals on the Internet. The other criminals used the credit card and bank information to buy goods on the Internet. To avoid being caught with stolen goods, the Internet criminals hired people to receive the packages, relabel them, and mail them to Russia or any other country in which the Internet criminals could easily access the goods. The “reshippers” hired were low-income individuals with U.S. addresses who responded to “work at home” ads posted on legitimate job sites. They were paid by the package. An extremely small percentage of these individuals alerted the authorities because they were concerned about being complicit in the crime.<sup>7</sup>

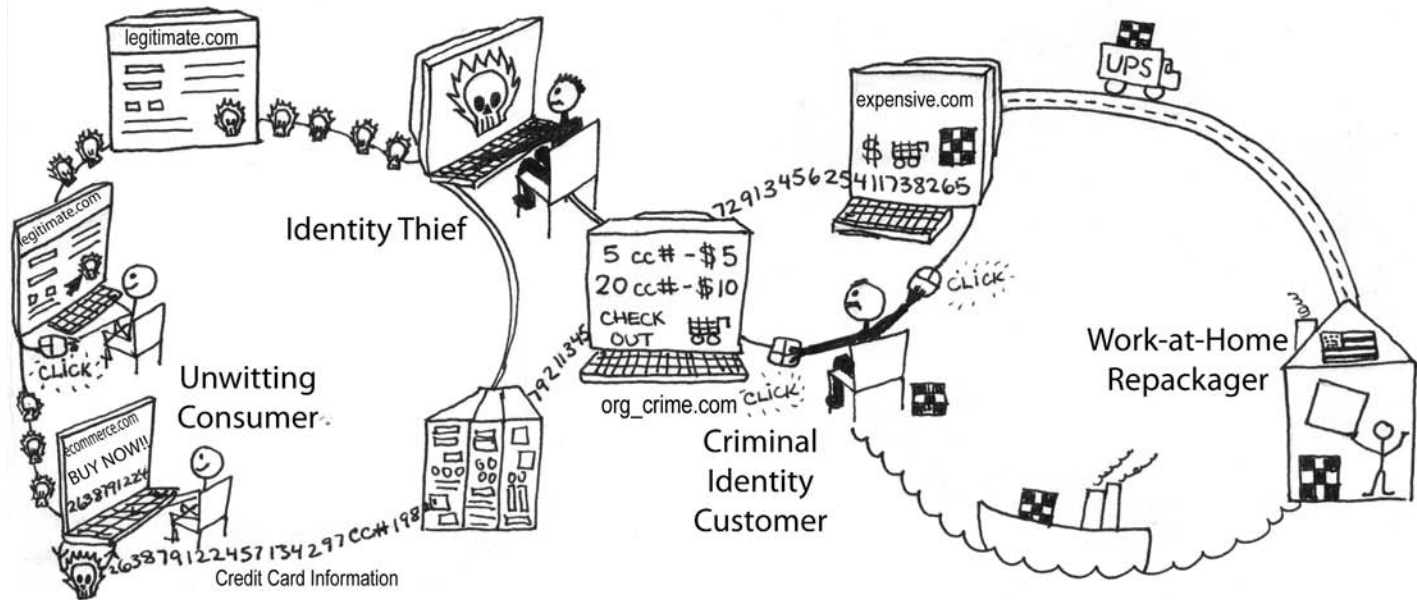


Figure 2-3: SHS7

The preventable aspect of this horror story is that the vulnerabilities that allowed the criminals to take over hundreds of legitimate business Web sites and thousands of users' computers had been identified years earlier and the patches were readily available. Although the electronic commerce sites that take credit cards are the vehicle in SHS7 by which money is stolen, anyone's computers that are connected to the Internet are targets because the attackers simply want to harness all possible computer processing power. In this case, the victims are not only thousands of faceless identity theft victims, but dozens of legitimate, blameless Internet commerce sites that eventually had to make restitution to the identity theft victim. There are also cases where widespread vulnerabilities can be used to launch very specific attacks. SHS8 describes one variant of these attacks. Again, it is a multi-step scam that may be better understood with reference to the corresponding diagram (Figure 2-4).

**SHS8:**

---

Similar to the scenario in SHS7, organized cybercriminals, this time from Britain and Ohio, planted software on unsuspecting Web users' computers. Rather than capturing data, this software allowed the criminals to control the computers remotely. Via a remote command, they could instruct the computers to send massive amounts of connection requests to any given Internet site. The criminals then sold time on these computers to the owner of a home satellite retail business. He directed them to flood the Web sites of three competitors with connection requests. The competitors' Web sites were essentially shut down, and they lost more than \$2 million in revenue and cleanup expenses.<sup>8</sup>

The "flood" in SHS8 is an example of using one set of computers to shut down another set. This causes the victim computer to ignore requests for information services from legitimate users of the victim computer, so it is called a "denial-of-service" attack. Again, the preventable aspect of the SHS8 horror story is that the vulnerabilities that allowed the criminals to control the victim computers had been identified years earlier. This story is the same as SHS7 in that there is no specific target profile for the compromised computers. It differs from SHS7 in that there is a specific unique target in the ultimate victim's home satellite retail Web sites. More-

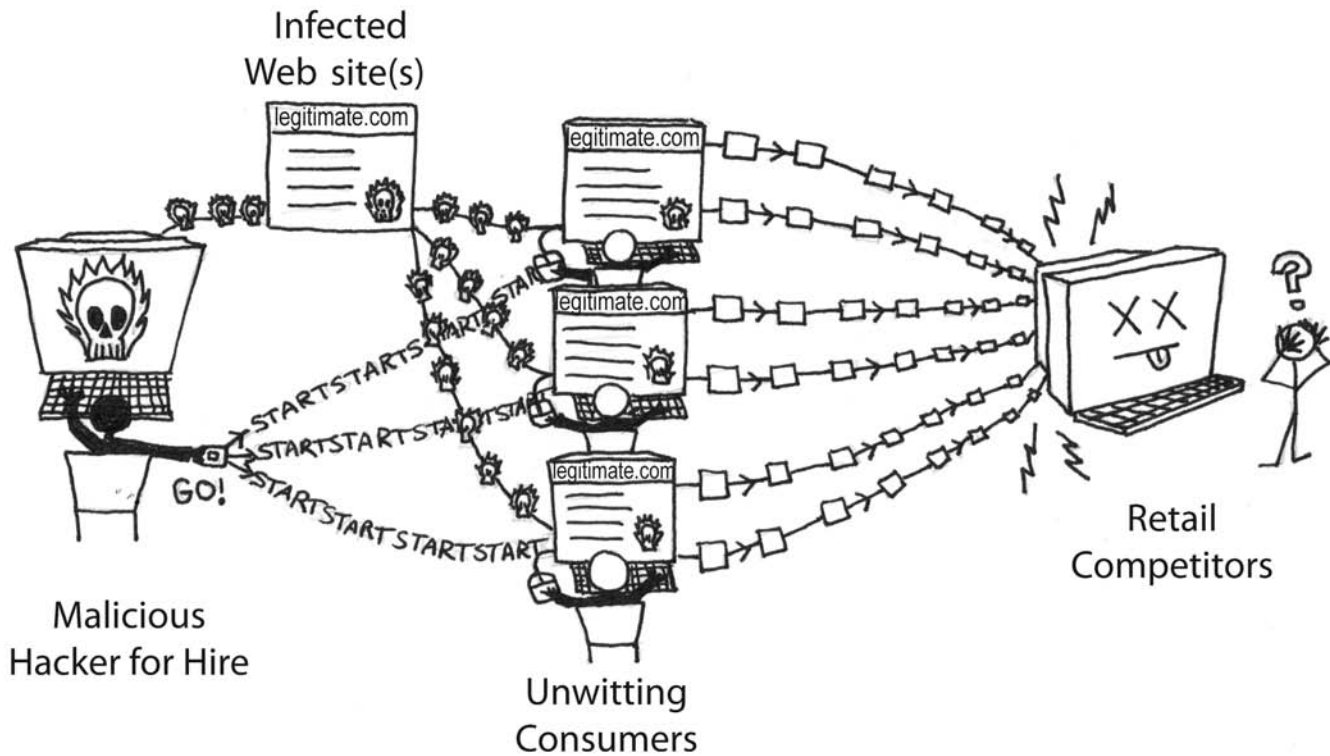


Figure 2-4: SHS8

over, these could have had perfectly reasonable security, but there was nothing they could have done that would have prevented the attack. A similar attack was directed against multiple U.S. government and financial services sites in July 2009; this attack is widely believed to be an act of cyber war.<sup>9</sup> As in the case of a suicide bomber, some threat to assets cannot always be prevented, and even identifying the threat source in the act of the crime does not help victims protect themselves. Organizations are vulnerable to this denial-of-service cyber data storm the same way their physical assets are vulnerable to tornados.

As discussed in Chapter 1, a CXO should not view information about potential threats as a source of FUD-factor recommendations, but in the context of due diligence with respect to asset preservation. A critical piece of information in evaluating the adequacy of security over assets is the landscape of potential threats. Checking out the threat landscape is never a fun experience. No one is comfortable thinking about who might be motivated to steal, damage, or destroy assets. Few victims in any security horror story ever thought they were targets before actual harm was done. However, without some glimpse of threats and vulnerabilities in your asset landscape, leadership in security will be an elusive goal.

Figure 2-5 is an example of a threat landscape. Notice how it dovetails with the asset landscape from Figure 1-1. The security horror stories in this chapter have prompted ideas for threat inclusion. In addition, the threat landscape in the figure acknowledges that threats could even be environmental, like weather and power outages. In some sense, everyone faces the same threats. A good security professional can recite the common ones without thinking. The role of the CXO in building a threat landscape is to concentrate on threats unique to the organization.

If in an asset landscape there are the uniquely valuable items that differentiate an organization's products or services from any other, there are probably unique vulnerabilities and threats as well. It could be value related to expertise that is threatened by turnover or retirement. It could be a valuable supply source that is threatened by vendor resource constraints. The reason the threat landscape overlays the asset landscape is to allow a realistic view of where and how security might be needed.

## THE SECURITY PROGRAM

The topic at hand is value preservation. If a branch office getting struck by lightning does not affect the value of the business, then the organization may not consider weather a threat. Threat landscapes focus on threats

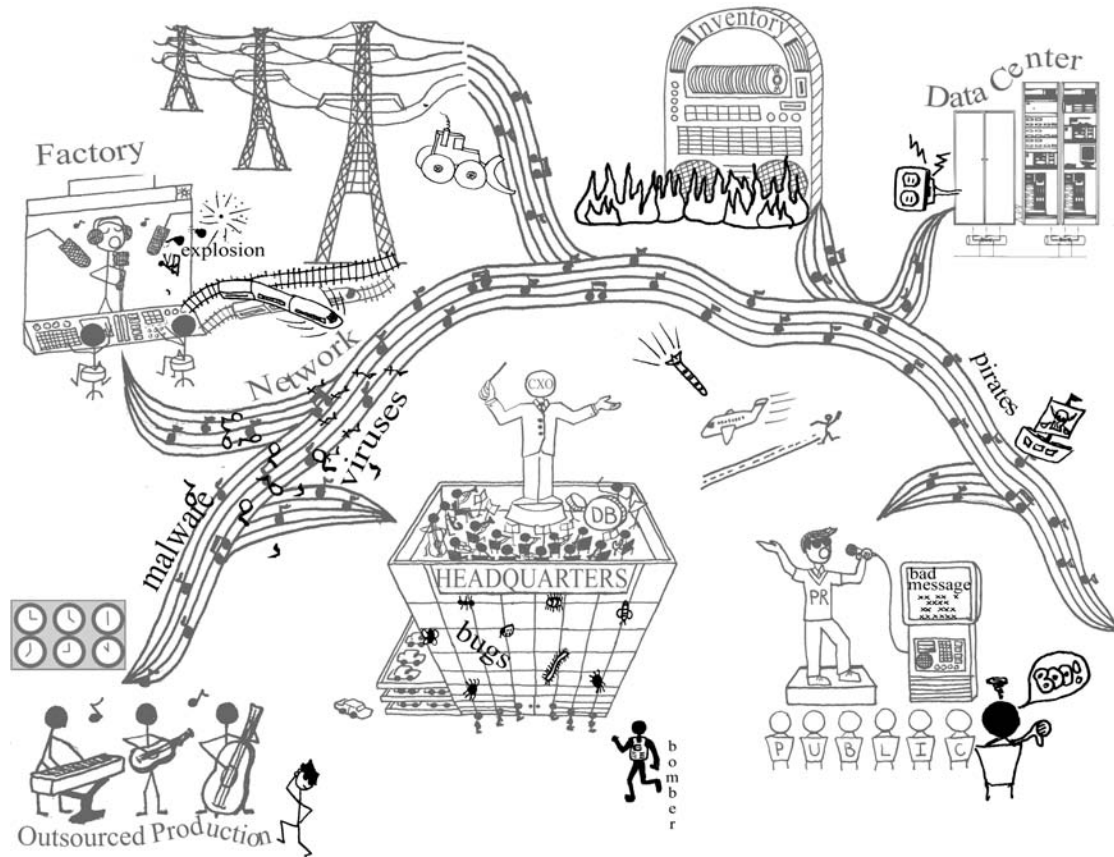


Figure 2-5: Example of Threat Landscape

that impact value. The threats should be envisioned regardless of whether there are restrictions or monitoring of a perimeter around the assets. Whether or not a threat is successful will depend on a variety of factors, some of which may currently be unforeseen. So it is appropriate to paint a threat landscape regardless of the situation with respect to the restrictions or monitoring that would prevent or deter someone from enacting a threat.

Once the threat landscape is fairly complete, a CXO's initial reaction to it will be to consider whether it is possible for the threats to be enacted. Take the simple example of threat of theft of equipment. Given the current set of security controls around a given asset, determination should be made on whether a foe would be able to accomplish that harm. The answer is yes only if the assets are vulnerable. Of course, there are degrees of vulnerability. An asset in a locked storeroom could be stolen by enacting a threat with a crowbar. So the asset is vulnerable. But if there is a situation in which the storeroom is left unlocked, then that situation presents a higher degree of vulnerability than the one in which the storeroom is locked.

Of course, a CXO is well aware that a threat plus a vulnerability does not equal damage. In order for a combination of threat and vulnerability to result in damage, the vulnerability must be exploited to enact the threat. Therein lies a security decision. Thinking about vulnerabilities often changes over time. Prior to the US Airways Airbus landing in the Hudson River in January 2009, it was known that birds can stop plane engines, but there was little recognition that anything needed to be done about it. The probability that the bird threat would be enacted simultaneously on both vulnerable engines was thought to be too low. Security risk management is an ongoing process of anticipating, understanding, and acting with respect to threats. It requires an understanding of how threats impact the business, an understanding of the current level of asset vulnerability, and proactive management to mitigate the vulnerabilities to an acceptable level.

A CXO may or may not be in a position to envision the full threat landscape or associated vulnerabilities personally, but should know that some individual has correctly incorporated the correct business impact estimates into the analysis. The holistic approach to designing security measures has long been considered best practice (in the credible sense of the term), and so a common, as well as regulatory-required, approach in many industries is to establish a Security Program.<sup>10</sup> The idea of a formally established Security Program is to ensure that the organization does not rely just on trust to ensure employees are protecting assets, but on a shared

organizational framework and trustworthy process. An adequate Security Program provides effective protection against obvious threats to the asset landscape.

Depending on the size and culture of the organization, the individual who runs the Security Program may be a dedicated resource or a manager who is close enough to the asset landscape to be able to understand its vulnerabilities. In coming to terms with vulnerabilities, the individual should be using real data that directly corresponds to the asset landscape. For example, if there is a substantial amount of confidential data stored in branch offices, then the individual who is evaluating the vulnerability related to data-theft threats should be knowledgeable with respect to branch offices. Furthermore, the individual should be in possession of concrete facts with respect to the branch office's information infrastructure. Those facts should include, but not be limited to, a network diagram, building layouts, personnel schedules, data flow, and associated protective measures. If the individual is performing risk analysis with just spreadsheets and surveys, the results should not be trusted.

It is also important that a CXO identify those in the organization who have a good sense of asset value and business impact, and require those people to participate in the design of the threat landscape. Everyone who is a stakeholder in preserving the asset value will have an opinion. A CXO who can persuade top lieutenants that the security landscape vision is important to accomplish will have a strategic advantage in accomplishing security goals. As security goals preserve assets, this translates to business advantage.

It is unfortunate that many CXOs and their lieutenants have experienced poor and expensive Security Programs that make them wary of time spent in security vision exercises. Opinions may be based on years of experience with Security Program managers who knew little about assets, and instead used checklists and spreadsheets to determine what security measures should be taken. Such cultural viewpoints can only be overcome with tone at the top. A CXO needs to make sure that key stakeholders understand that an incisive Security Program is a constructive approach to a complex problem, that they are accountable for getting it right, and that they will benefit from participation in the solution.



## CHAPTER 3

# TRIAD AND TRUE

A CXO with a good handle on the threat landscape may nevertheless have only a vague idea of whether assets are actually vulnerable to threats. Figure 3-1 depicts the threat landscape of Figure 2-5 overlaid with security measures. The security measures are designed to minimize the impact of threat exploits, but they are not sufficient to render the landscape invulnerable. A vulnerability analysis is like a puzzle overlay on the threat landscape. In this analogy, the puzzle pieces are security measures that minimize the impact of threats, and missing puzzle pieces are gaps in security measures that leave assets exposed to threats (Figure 3-2). Even a CXO who understands the complete puzzle may not always be comfortable with it. Comfort levels change with changes in the landscape. At times, the comfort level will be low, and a CXO will be motivated to communicate about it. Using whatever tone is normally employed to communicate on important initiatives, the message should be unequivocal: “We need to have security.”

Where there is the ring of true *tone at the top* in the message, the rank and file will believe that the message is actionable. But they will most likely still look to the CXO’s direct reports for guidance. If the direct reports show no understanding of what “having security” means, neither will the rank and file. So, in addition to the unequivocal message, there may also need to be some support and counseling. A CXO should encourage all staff to identify the assets they rely upon to do business and to identify security processes that have been put into motion to secure those assets.

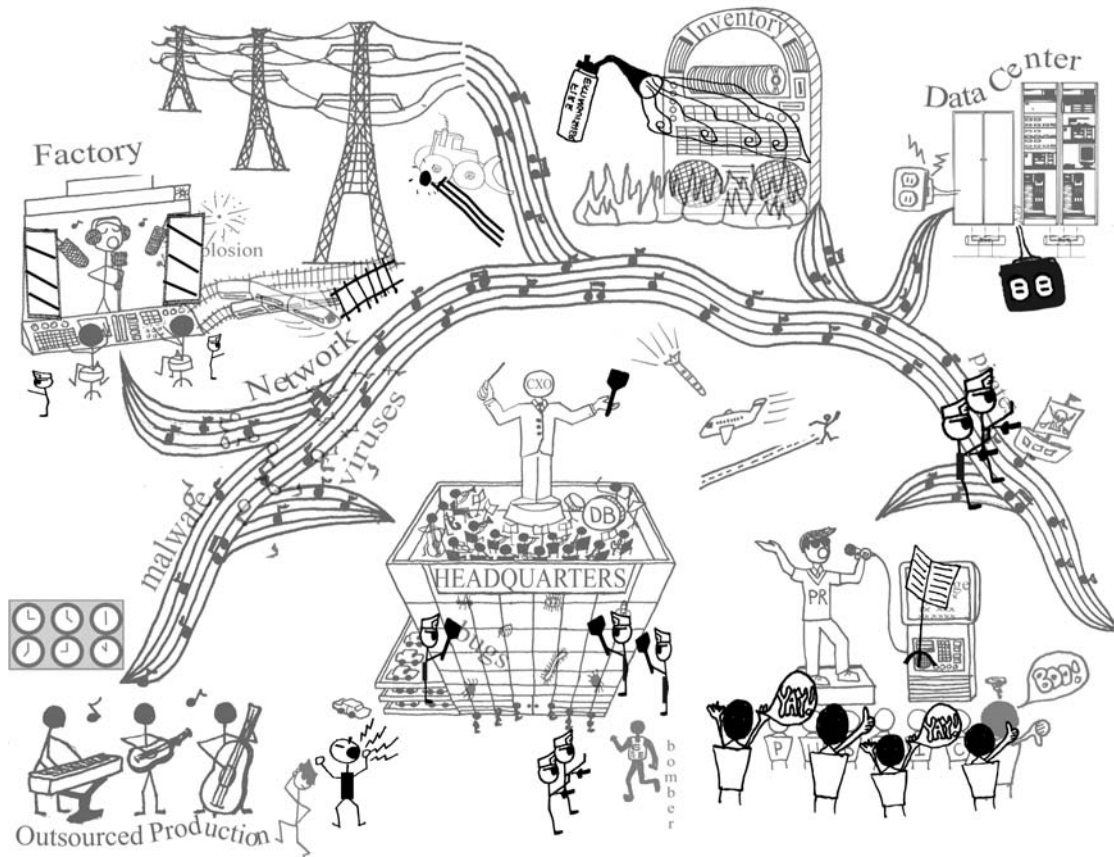


Figure 3-1: Security Measures

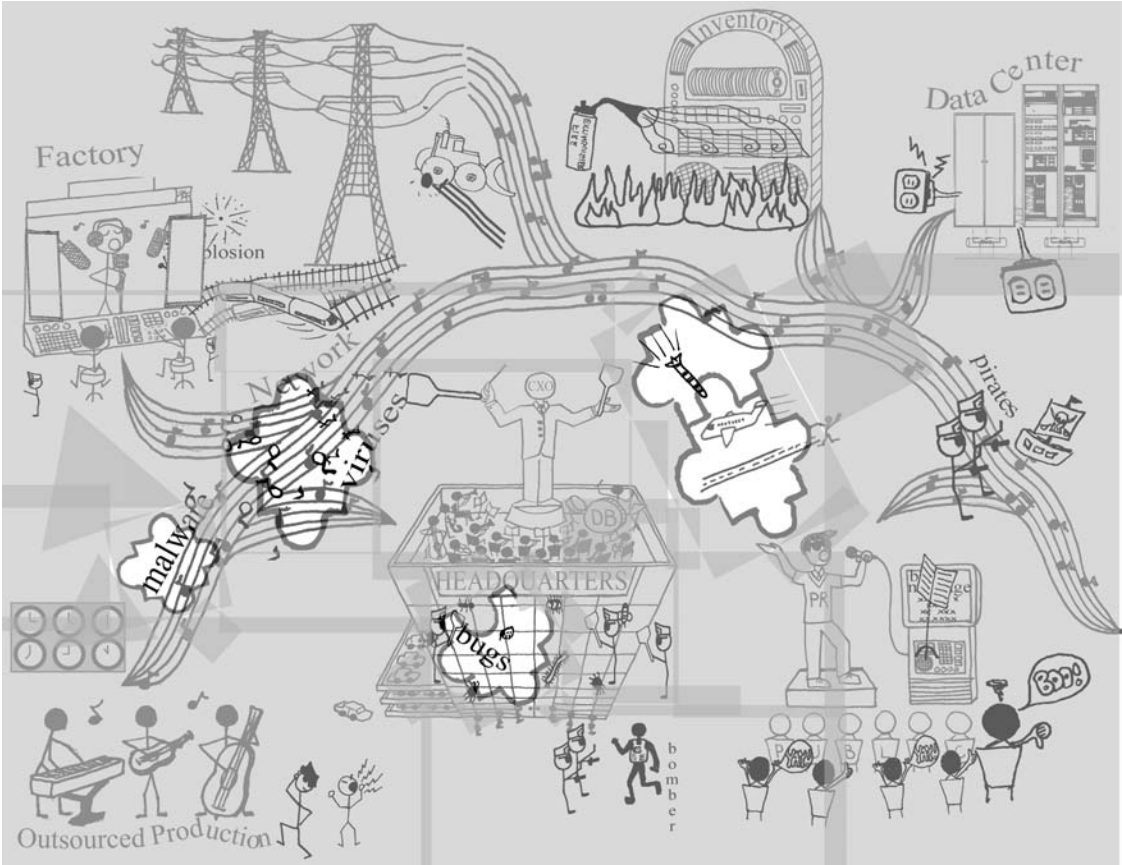


Figure 3-2: Security Puzzle

It is key to make sure that managers know they are responsible for actively managing security processes. If an organization is not managing security processes, then the security processes are managing the organization. In effect, any individual who establishes a security process has been given some power to affect the behavior of the rest of the people in the organization. That individual is making others choose passwords, show badges to guards, fill out forms, memorize combinations, and a variety of other inconveniences. Where security measures are occurring within a management domain, the managers in that domain should be held accountable to demonstrate that the security measures have a positive effect on minimizing the impact of threats to the asset landscape.

## PREVENT, DETECT, RESPOND

Visible security measures such as signatures on forms are called *control points*. Control points work only when they are managed well. They should be chosen in the context of a management process specifically designed to secure assets. Simply requiring a form to have an authorization signature is not a control point unless there is a process whereby a false signature would be caught. Assuming someone did falsify a signature and the forgery was caught, there should be a well-defined management process to correct the violation, as well as recover the value of any lost asset. Control points make sense only in the context of a management process that includes those three key steps: prevention of harm, detection of harm that is unfortunately not prevented, and response to harm once it is detected. Otherwise, the measure is only “keeping your friends out.”

The recognition that prevention, detection, and response processes are the keys to any successful security process has made *Prevent, Detect, Respond* a mantra among security professionals. It has given rise to a number of visual representations such as the one in Figure 3-3. The arrows in the figure indicate that the response process should also include a feedback loop. The feedback loop representation dictates that the response process include an investigation into why a control point failed to accomplish its intended mission, and information gathered in that investigation should be used to strengthen prevention and detection processes. Figure 3-3 shows the relationship between the three types of control points as they interact within security operational process.

The loop may look similar to the security management cycle in Figure 1-2 introduced in Chapter 1. But the prevent, detect, respond cycle

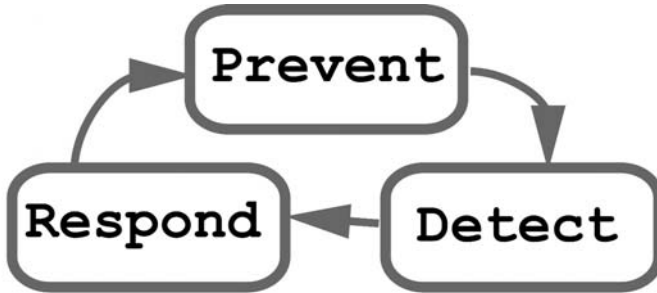


Figure 3-3: Prevent, Detect, Respond

does not depict management strategy. It depicts operational process. The prevention-detection-response cycle sits within the security management cycle, as depicted in Figure 3-4. Although some security literature may blur the distinction, the prevention, detection, and response cycle differs from a security management process in that it covers only

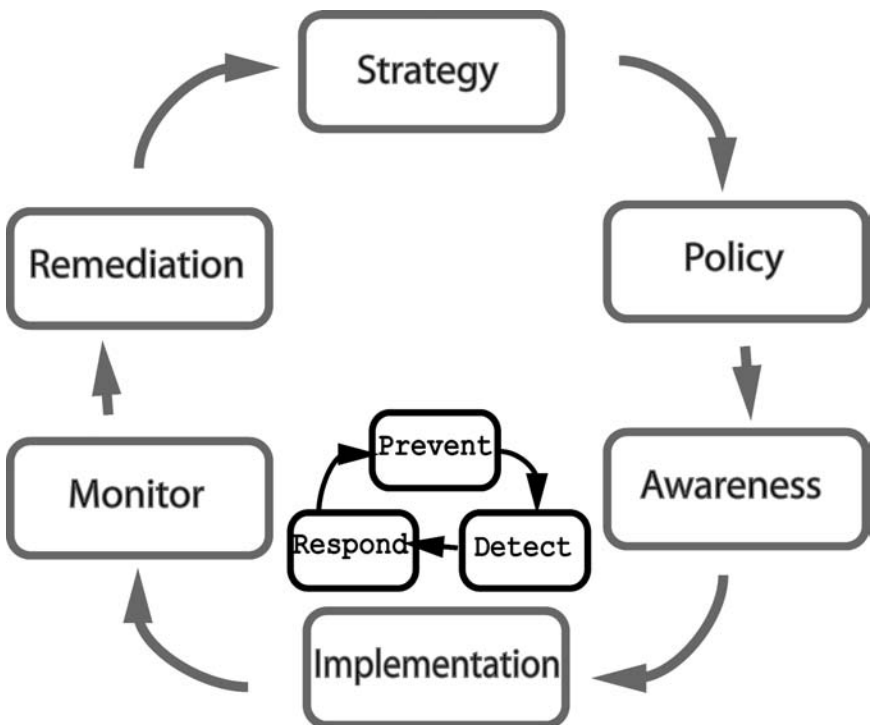


Figure 3-4: Cycle Overlay. Adapted from Bayuk, Jennifer, *Stepping through the Security Program*, ISACA, 2007.

the operational side, not the strategic side, of security. Prevention, detection, and response are the day-to-day operational processes that are set into motion by a more comprehensive and strategic security management process. They represent the combinations of measures chosen by management to ensure that security is an attribute of the assets managed by the organization.

This sequential triad: *prevent, detect, respond*, has multiple variants in security literature and is often phrased in a rhyming form: *prevention, detection, correction*. The word *correction* is substituted for *response* to indicate that whatever vulnerability may have been exploited to bring operations into response mode is a vulnerability that requires correction as part of the response process. Security operational process is also described in terms whose shades of meaning specify various aspects of each triad component to security professionals. Such words as *avoid, deter, mitigate, alert, recover, investigate, and remediate* indicate subtle differences in the way prevention, detection, and response are performed. For example, one can implement processes that make an asset less of a target by lowering its value. A good example of this type of security measure is the dye-filled tags used by the retail industry to deter clothing theft. They require special devices to be removed without dye ruining the clothing. This has an effect similar to a preventive control in that it lowers the probability that a threat will be enacted. Nevertheless, the cyclical prevention-detection-response triad will, for simplicity's sake, be used herein to mean the operational combination of people, process, and technology that keep assets secure on a daily basis.

A CXO who is keeping an eye on the security management cycle should be able to count on staff to maintain security operations cycles. It is only when standard-response operational processes do not work that incidents are escalated to the management cycle and are targets for remediation at the management process level. Even then, not all analysis of remediation activity will trigger changes in security management at the strategy level. The idea is that some security requirements have no easy prevention or detection strategies, and security operations will necessarily rely heavily on the response mechanism.

A good example of this is desktop security. There are so many bad things that can happen to personal computers nowadays that it is very rare for a security process to have adequate prevention capability. Consider the situation in SHS9.

**SHS9:**

---

The act of doing business on the Internet corrupts the integrity of personal computers in ways that avoid detection. A user in a marketing department, doing research on advertising companies, browsed through Web sites that contain example ads. Unbeknownst to her, a criminal posing as an advertiser purchased space on the page she is browsing, and used it to install malicious software. She clicked on the criminal's ad, and unwittingly installed a program that provided the criminal control over her computer.<sup>1</sup> The criminal proceeded to use her computer to commit attacks like the one described in SHS8. Eventually, the user complained to a technician that her computer was slow. The technician conducted an investigation and found the malicious program. The technician did not know where the malicious program came from, or the extent to which it could further infect the company's network. So, following response procedure, the technician did not attempt to remove the malicious program, but instead restored the functionality of the personal computer. The response was performed by wiping the file system and memory clean, and reinstalling all the business software so that it appeared to the user as if it was new. The user immediately saw that all the files that she had stored on the computer were gone.

Note that SHS9 is only a security horror story because the user lost files—information assets that were presumably valuable to the business. As the definition of SHS includes the term *preventable*, this was the only preventable aspect of the damage to the asset. There is nothing a security professional can do today to prevent harm to computers in an environment where end users must have the capability to experiment with new Internet-accessible software in order to do their jobs. So the information assets were not protected. Though it is possible to fully monitor all computers on a network, the extent of monitoring required to detect a random download is extremely resource intensive, and thus very expensive. Moreover, because the malicious code often is delivered via a legitimate-looking advertisement, the expenditure would provide very little in the way of reliable detection capability. So the major security mechanism in the triad for the personal computer arena is the last resort: response. The reason this is

a security horror story is that all security professionals should know that personal computers attached to the Internet should never be relied upon to store files or other valuable data. In an environment where it is well known that files on personal computers are at risk of being lost due to response processes, there should also be mechanisms whereby those files are stored in a recoverable format outside of the user's personal computing environment. Sometimes that control point has to be achieved in cooperation with the computer user. Simply to generate awareness that important files must always be stored on an enterprise server rather than a personal computer would be one step in that direction. Requiring users to follow a systematic approach to storing and labeling business-related files would be one step better. This is a reason why the prevention, detection, and response portion of the daily operational cycle sits in an area in Figure 3-4 that includes the awareness portion of the management cycle. Well-trained people are an important component in the daily security operational process.

## CONFIDENTIALITY, INTEGRITY, AVAILABILITY

Of course, the evaluation on whether a prevention-detection-response triad efficiently or effectively meets requirements is entirely dependent on having a good set of fairly low-level technical requirements that fill the gaps in the vulnerability puzzle. Security *requirements* are usually framed in the context of another triad: *confidentiality, integrity, and availability*. In the context of a security requirement, *confidentiality* refers to the ability to restrict contact with assets only to those with a need to handle them. *Integrity* refers to the ability to isolate assets from tampering except by those who are directly responsible for maintaining the asset's value. *Availability* refers to the ability for authorized individuals to have direct access to assets when they need it to execute business process.

As with the prevent, detect, respond triad, there will be those who annotate the confidentiality, integrity, and availability triad with alternative expressions, such as *authenticity, completeness, control, possession, secrecy, utility, and validity*.<sup>2</sup> These subtle distinctions are most often encountered in the context of cyber security. For example, it may be required that given constituencies possess information, but use it only for a specific purpose. This is a *utility* requirement. It may be required that an information asset be validated as coming from a given source. This is an *authenticity* requirement. For purposes of discussion, these requirements will collectively be referenced using the confidentiality, integrity, and availability triad.



Confidentiality, integrity, and availability principles apply equally to information and physical assets. Requirements for confidentiality have given rise to a multitude of electronic access control devices as well as physical container technologies for paper and electronic media. Requirements for integrity have been instantiated in data management systems, as have physical maintenance measures. Requirements for availability have spawned a wide variety of data center technologies as well as personnel and inventory protection profiles. Note that while confidentiality, integrity, and availability as requirements may apply to both information and physical assets, information security is often referred to as *logical* as opposed to *physical* security to highlight cyber-specific aspects of the requirements.

From the point of view of a CXO, security has historically been dominated by the availability requirement. Though recent enforcement of privacy laws have somewhat increased the emphasis on confidentiality, the primary purpose of security, most would agree, is to ensure that facilities stay functional, inventory is available, and information technology is redundant and fully recoverable. These are requirements on the *availability* side of the triad. Whether or not a CXO appreciates confidentiality and integrity will depend on experience with how these requirements were met by the Security Programs in the past. Some CXOs' past experience with security process has led them to associate confidentiality and integrity with overly restrictive and ineffective, and thus useless, control points.

Nonetheless, even in environments where there are no confidential secrets, availability cannot be achieved in isolation. Availability depends on methods to ensure that unauthorized people are not provided with the information they need to get access to assets, this information restriction requirement is met by reference to confidentiality requirements. For example, passwords must be kept secret to be effective access control tools, and access control is necessary to provide availability. Availability also depends on methods to ensure that response mechanisms actually work as expected, which is itself an integrity requirement. So no real Security Program can accomplish anything unless it has the capability to address all three requirements in the triad.

Especially in the context of cyber security, availability is heavily dependent on minimizing the need for access to information systems to select trusted people (i.e., achieved through meeting requirements for confidentiality). It is also extremely dependent on accuracy of the data at the back-up or alternative site (i.e., ability to demonstrate that the data meets requirements for integrity). So even CXOs who place primary importance

on availability must, out of necessity to fulfill the mission, support a Security Program that includes confidentiality and integrity objectives. In order to meet any security objective, the scope of the Security Program may not be limited in scope to any one aspect of the full triad.

Of course, not all assets will require a level of security that aspires *equally* to all three objectives. Nevertheless, the triad helps frame requirements on an asset-by-asset basis. For example, say one asset is an Internet Web presence. It must have integrity and be available, but the information on it will not likely be required to be kept confidential. Confidentiality requirements may be limited to the passwords that allow someone to change the content. Day-to-day management communications via email, on the other hand, should be kept confidential; but unless there are legal or regulatory requirements to keep records of it, it may not be required to be available for long periods of time. The email system itself, by way of contrast, must have integrity and availability, and its administrative and user interfaces should be kept confidential.

Despite the ability to relax requirements on one side of the triad, the basic ability to establish control points for confidentiality, integrity, and availability is the core competency of any Security Program. A Security Program should be able to meet confidentiality, integrity, and availability requirements at the physical and logical perimeter around the organization itself, and also around any distinct asset, including information, even when it is widely distributed, as is the case when information must reside on mobile devices. Without this capability, the program is destined to fail. There should be no debate over whether a given asset perimeter is within the boundaries of a Security Program's scope. The only questions should be to what extent there are confidentiality, integrity, and availability requirements for those assets, and whether there are resources to meet those requirements.

## **PEOPLE, PROCESS, TECHNOLOGY**

A Security Program that has the basic ability to implement and maintain security control points to meet any security requirement should be able to gain economies of scale from the management process by which the control points are maintained. Where this fundamental management process and core capability have been established, security measures can be ratcheted up, as needed, to meet new business requirements introduced by a changing threat and vulnerability landscape. Security measures are combinations of people, process, and technology that are coordinated to achieve security objectives.

The need for a baseline level of security competence is the reason why a CXO who is not comfortable with the vulnerabilities on the asset landscape needs to say to the leadership, “We need to have security,” rather than, “We need to manage security risks.” There will always be debate about how much security is enough to provide reasonable assurance that risks to assets are minimized. There is no need to start out by inviting the debate on whether a Security Program itself is necessary. Security controls are very hard to establish within an organization. If the organization perceives the chance to debate whether a whole program is necessary, the effort will be strangled before it can get started. The goal must clearly be to secure the assets. Staff should be directed to strive toward that goal. If security measures that are recommended in response to the call seem too risk-averse, the CXO can make that call. But in the absence of a working Security Program, even small security measures cannot be implemented on an organization-wide basis.

A security professional should be able to make basic decisions on where the risk/reward trade-offs are in general cases. This is true because, to some extent, everyone faces the same threats. There are many readily available security measures from which to choose. Entire professional organizations and international research teams have contributed to the literature on what works and what does not when it comes to implementing security measures. There is well-documented authority on how physical security professionals should estimate the strength of office defenses against potential workplace violence, so once the requirement to reduce potential for workplace violence is adopted, no one should want to question competent security staff in following the associated best practices.

On the other hand, the plethora of security literature also has a downside. It has inspired some security professionals to adopt a checklist approach to implementing security. It has also motivated some security professionals that do not fully understand business requirements to implement the wrong security measures. In the worst of such cases, a best practice document is selected, and a Security Program is designed around the document instead of around the asset landscape; the security professional declares compliance with an international standard and challenges anyone to find fault in the execution of security due diligence.

Every CXO should be aware that, although best practices and guidelines are useful training materials in the security realm, and can lead to some good decisions in commonly faced scenarios, there is no consensus in the security literature on how anyone should decide which combination of people, process, and technology are best suited to achieve a security management

objective. There is no evidence that compliance with any published best security practice reduces risk to an organization that follows it. Quite the reverse: there is plenty of complaint in the security literature that those who adopt best practice management standards often are lulled into a false sense of security.<sup>3</sup>

Nevertheless, where security professionals have educated themselves on internationally recognized security standards documents, and are employed to apply best practice to the organization's unique landscape, a CXO should be able to state business requirements for security in plain language, and expect the security professionals to accomplish a baseline level of security operations that covers the asset landscape in an efficient and effective manner. These requirements will be asset-centric confidentiality, integrity, and availability requirements.

Business requirements are referred to by security professionals as *control objectives*. A control objective is defined with respect to security the same way it is defined with respect to any other management function: as a statement of the desired result or purpose to be achieved by implementing management control over a particular activity. Actual combinations of people, process, and technology implemented should produce *control activity* in support of a control objective. Where the activity exists, it will include control points. The control points should be evident, and this *evidence* should provide the basis for both management *metrics* for and *audit* examination of a Security Program. It is the job of the security professional to map control objectives to process and measurable control points.

Anyone who reaches CXO level already has leadership strategies in place to accomplish management processes like these. A CXO must merely apply them consciously to security. A CXO must evolve security strategy into policy, understand in general how control activity in support of the policy is supposed to work and who is supposed to be doing it. A CXO should enable the security staff to track accountability for control points using some method of independent evidence collection. Assuming this evidence has integrity, it should be turned into metrics that are used make decisions. Most importantly, a CXO must connect security audit results to the overall strategy, not necessarily only to the control activities from which audit evidence is typically collected. Figure 3-5 illustrates this theoretical progression in the form of a blossoming security program.

Efficiency in managing security measures is all about making the broadest possible use of every control activity to contribute to multiple control objectives. Therein lies the real quandary in implementing any kind of security triad. On exactly what should security dollars be spent?

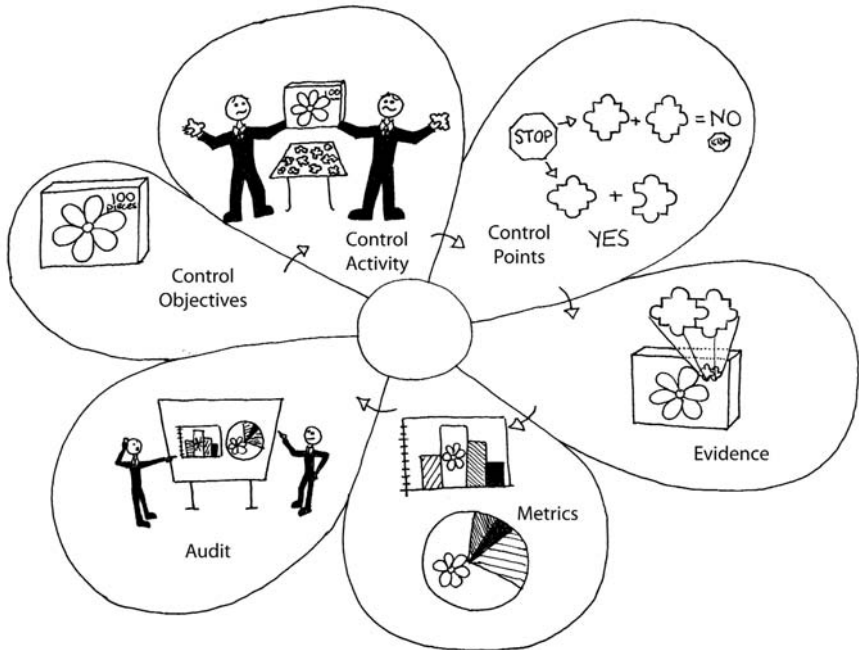


Figure 3-5: Control Lifecycle

Which combination of prevention, detection, and response security measures will cover the most confidentiality, integrity, and availability requirements? The answer is not clear-cut because any Security Program has to have some basic operational capability to accomplish even a single prevent, detect, respond measure to meet a single confidentiality, integrity, and availability requirement. Organizations that have not spent any effort on a Security Program usually face situations similar to SHS10.

### SHS10:

A new CEO has been hired to take a profitable private company public. On paper, the business looks very healthy, and he accepts a given target date of three months. He takes the precaution of bringing in independent financial consultants to find and fix any accounting irregularities that may not meet regulatory scrutiny. After a few months, the financial consultants discover that they cannot rely on the integrity of the accounting information systems, and they advise the CEO to bring in a technology consultant. After a few weeks on

the job, the technology consultant confirms that there are data entry and aggregation inconsistencies, but advises the CEO that the root cause of the problem is lack of accountability due to poor identity management. There is no authoritative list of employees and contractors at the firm, and no way to automatically produce one. Payroll lists are updated only every two weeks. Every branch has its own payroll system. There is also no central contractor or vendor registration. There is no dedicated security staff. Rather, multiple facilities and technology departments provide access to buildings and systems upon request from any current staff member, employee, or contractor. The facilities and technology departments are only sporadically informed when people leave the firm. The company has a dozen individually operating business units, and none of them have responded to requests for a currently active list of users. In addition, systems contain hundreds of generic user accounts that are not associated with individuals, but instead tagged for IT-only usage. These presumably may be used to run automated processes or to provide access for temporary personnel, but there is no way to verify the usage. Many of these accounts have administrative access to various systems. The consultant further advises that there is no way to easily fix the problem. Even if lists of authorized users were to become immediately available, there is too much risk to the business operations in closing down the unclaimed accounts in a short timeframe. In particular, investigation into the necessity of the generic accounts would likely take months. Moreover, the problem would be fixed only for that moment. As soon as the businesses requested access for new personnel, the problematic situation would regenerate. The consultant advises that, without simultaneous effort on both remediation work and the establishment of an ongoing identity management strategy, the firm will be unable to demonstrate management control over assets, and so would fail external audit. The CEO is left to consider whether to delay the public offering until a Security Program can be put in place.

In the context of SHS10, consider the basic Security Program control objective that only authorized staff should be able to walk unescorted in company office space. This control objective requires that the definition of authorized staff be very clear. No matter what technology is purchased

or people put on the job, it will be impossible to accomplish this objective without an identity management system. On the logical security side, consider a control objective that only authorized staff should be able to access the general ledger. Even if the list of authorized people who can access the general ledger could be determined, the presence of generic administrative accounts opens the door for virtually anonymous and undetected access.

Another example of a basic Security Program control objective is a requirement that all critical business applications have back-up. Prerequisites for achieving the objective are an *inventory of business applications* and a definition of *critical*. Organizations that do not have a basic Security Program are *unlikely to have either*.

Unfortunately, people who do not have security experience tend to take such fundamentals for granted. They will scornfully comment, “Just get the list of employees from payroll” or “Just get the list of applications from IT.” But it is just not that easy. SHS10 illustrates that, where a payroll department has no requirements to make a list of employees available to the rest of the firm on a daily basis, there is no expectation on their part they should need to do so. Also note that an IT department can be just as scattered as the business unit branches in SHS10, and there is truth to the saying *if you really want to screw things up, put them on a computer*. A Security Program needs to have basic capacity to enforce *general controls* in order to accomplish any specific objective with respect to a single asset.

## AUDIT, REVIEW, ASSESS

*General controls* is actually an audit term. It refers to those basic capabilities a Security Program includes that apply holistically to the organization. The way for a CXO to approach a Security Program is, like the way to approach any management endeavor, top-down. It is to formalize an organization around the security management cycle in Figure 3-4, and assign formal responsibility to staff to do their part to get the required pieces in place to make it happen. The CXO must foster recognition that, in order to tackle any one puzzle piece, a Security Program must, in general, have a way to accomplish any given security requirement. If there are sections of the asset landscape where vulnerabilities can be eliminated with one or two prevalent control activities, then these are probably general controls, and there should be standard, best practice, and usually reasonable cost ways to achieve them. Only after general controls have been established is it possible to ratchet security standards up for specific systems or processes.

An assessment such as the one performed by the technology consultant in SHS10 will often produce a list of missing puzzle pieces. But the measures chosen by management to reduce vulnerabilities uncovered in an audit don't need to be individual puzzle pieces that are the same as the size and shape as the gaps. This would reduce all security measures to *countermeasures*. A *countermeasure* is just like any other *prevent, detect, respond* control except that the reason it is put into place is to reduce an asset's vulnerability to a specific type of threat. Countermeasures are sometimes implemented as knee-jerk reactions to threats, rather than as security enhancements that can be broadly applied. Wherever possible, comprehensive general controls should be established at the landscape level such that the security in place can be viewed as an attribute of each asset type within the scope of the controlled environment.

A solid Security Program that covers the full scope of general controls confines debate on implementation of security measures to the harder, more uncommon situations specific to the business of the organization. This should be the point at which the security management decisions may yield to risk management arguments. There is a huge amount of security literature devoted to "security risk management." Note that this risk management debate should never be over core components of the Security Program itself. The program should be organizationally functional and aligned with the business process to the same extent that a CXO might expect of a human resources or a building services department. The risk management debate should be over only the alternative implementation strategies to meet specific security requirements for which there are no current control points. The hardest job of the Security Program in filling in the remaining puzzle pieces is to understand what each recommended type of security control point will do to reduce those unique vulnerabilities, and whether it is worth what it costs.

A CXO must keep in mind that all the security management literature on how to make risk management decisions directs the security professional straight to the CXO office.<sup>4</sup> A typical security professional's objective in risk management is to reduce the variability between *expressed or implied risk tolerance* and current level of exposure.<sup>5</sup> The *expressed or implied risk tolerance* comes from leadership. Like the tone-at-the-top message for security itself, if there is no top-down communication with respect to risk tolerance, people may just make it up.

For example, say there is a call center operation that directly supports clients by answering questions about orders and resolving any delivery delays or misunderstandings. Those who are responsible for maintaining



the technology it needs to operate should be told something about the dependency of the business on its operation. To meet availability requirements, it must have a robust fault-tolerant mechanism. So two of the most significant control objectives a CXO may set for call center management are the *recovery point* and *recovery time objectives* for the call center.

The *recovery point objective* is the complete set of information and physical assets required to restart an interrupted process with a comfortable level of integrity. The recovery point chosen should be the minimum infrastructure the business would need to resume operation. The *recovery time objective* is the time it takes to get the process back up and fully functioning after it has been interrupted via some unforeseen fault, or intentional damage to assets. Normally, it does not pay for a CXO to learn tech-speak in great detail. However, because availability of business process is a key concern, these are good terms to know. If these objectives are not set with the business process in mind, they nevertheless exist, and the response process may be much less robust than the business expects.

A CXO may specify that the recovery point should be at least 25 service desk staff answering the 800 number with access to the customer records database and the recovery time should be less than 15 minutes. This may seem the obvious answer to the CXO with respect to the call center. At the same time, a CXO must be careful not to make any sweeping remarks about recovery points and times that could be misinterpreted and generalized to extend the decision concerning the call center to other, dissimilar assets. The recovery point objective for an accounting process wherein the general ledger system updated monthly may be month-end, and the recovery time objective for the general ledger may be a few days.

There are many alternatives to achieving security requirements for recovery point and recovery time objectives. Both the call center and the general ledger requirements could be met by having duplicate data centers with redundant systems and full-time staff in two geographically distinct accounting and call center departments, respectively. That plan may make sense for the call center. However, that level of effort would not be justified by business requirements for the general ledger system. A less expensive plan could be to make a post-month-end copy of the general ledger system and store it in an alternative location. That location could be configured to allow a quick install of the copy if it was needed, and accounting staff could fly in from other offices until a more permanent solution could be devised. This plan could be accomplished in a few days, be much cheaper, and still meet both recovery point and recovery time objectives.

Note that both plans require full buy-in from the CXO and department managers in order to be effective. Even though the general ledger plan does not have as much security, it is still a robust component of the overall Security Program. Each unique business process will have its own risk tolerance that will drive requirements for security control points. Only when clearly facing economies of scale does it make sense to consolidate diverse business processes under one set of common control points. For example, say the call center has 40 large machines replicated in its back-up data center. To add the general ledger machine as replication number 41 may be cheap compared to supporting a separate process for a back-up and restore process for the single general ledger machine. The consolidation decision has the potential to bring the general ledger system recovery up to 15 minutes whether it needs to be or not. However, the decision on whether to staff the second data center with accountants should still be reviewed separately.

Whatever the requirements, it is important to note that the availability requirement does not always have to recreate the asset landscape as it looked before the business interruption event. A CXO may opt for a response that does not include recovery of the damaged asset. For a simple example, where a building is lost to fire, response could involve outsourcing the business function that was housed in the facility, or selling that piece of the business. The recovery point is, in effect, nonexistent. Such a response plan might have a rather lengthy recovery time objective. But the choice is the CXO's.

Where it is obvious a business process relies on asset availability, a CXO should not wait to be asked what the recovery point and time objectives should be by a security manager. A CXO should make the requirements very visibly known so there is no debate when assets are lost over where the management lapse occurred. Consider that the technician in SHS9 did have an approach to security response. It was to recover the computer as an asset. However, the approach did not consider that the files were also an asset. From this situation, it can be inferred that the organization's Security Program included a control activity to recover the computer but not the files on it. Because it overlooked that type of asset, it left the files vulnerable to obvious threats. This is an example of a control objective that was not set by the business, but was nevertheless devised in the context of implementing a Security Program.

A CXO can catch this type of omission via an audit or a security review. A security audit or a security review is an activity by which management objectives for security are formally mapped onto control points within an organization, as in Figure 3-5. An individual examines all control activity

in great detail to make sure that the dots are actually connected as assumed. Some analysis is done as to whether the control points are adequate to meet the objectives. A report is issued that provides an assessment on whether the objective is met.

A CXO will often commission an audit or a security review in order to get an assessment on the level of exposure of a given asset, or the entire asset landscape. Like the choice of recovery point objectives, the choice of what type of audit or security review to commission is usually left to a CXO. The security management team may advise, but rarely makes the final decision. This is because the results of any given audit and security review may include recommendations for work in the security department. For a security manager to make a decision on the type of “independent” review may be perceived as either inviting trouble or providing a rubber stamp for the department’s work. Thus, like the alternatives with respect to recovery points, a CXO should understand alternatives with respect to independent security assessments.

The difference between an audit and a security review is that auditors usually do not report to the same management as the staff accountable for the assets in the scope of the audit. The word *audit* implies a truly independent assessment on whether assets are appropriately handled, and it is generally recognized that the staff directly responsible for maintaining the security in the environment under scrutiny cannot be objective in this evaluation. Certified auditors are guided by a code of ethics that prevents them from working on projects where their independence may not be obvious. Security reviews, by contrast, are often performed as part of the process of security management itself. They may be done by anyone within the organization and are often conducted or contracted by the organization who is attempting to implement security to see if they are on target.

Both security audit and security review activities, when done correctly, follow the same general process.<sup>6</sup> They both have a well-defined objective stated in management terms, such as, “Security over Internet Commerce Transactions.” They both have a well-defined scope, which is a subset of the asset landscape. They both have an agreed-upon approach, for example, automated testing of security configurations supplemented by staff interviews. They both are constrained by time, money, and the level of skill of the audit or review staff. Finally, in addition to the summary assessment of whether a management objective is met, they both produce “findings” in the form of lists of specific issues to be addressed.

The findings list in a security audit or security review usually describes vulnerabilities within the organization that are in conflict with manage-

ment goals for security around a given asset. Each finding is commonly accompanied by one or more recommendations to add control points to the environment which would reduce the probability that threats could be enacted which would exploit the vulnerabilities. Where recommendations are very specific to one type of threat to which assets are vulnerable, they describe countermeasures.

In many organizations, audits and security reviews are ordered by management immediately after experiencing a security horror story. It is easy to see how focus on a single security horror story can highlight a combination of vulnerabilities to the point where the security measure is specific to the threat most recently encountered. Nevertheless, security measures taken in response to one audit or security horror story are rarely designed to address the root cause of underlying vulnerabilities. Where the entire asset landscape is kept in view, it is easier to see how alternative security measures may cover more threat-vulnerability combinations than any single one uncovered in a security review.

Moreover, even for seasoned security auditors and reviewers, it is not always possible to foresee all the threats to which assets are vulnerable. So security measures should always be in place to detect harm that is not prevented. In 2007, a Microsoft security spokesperson said, "It's sort of like we've been in the medieval age of computer networking and access. And we say, you know, we just have to build more and more. So we build thicker walls, higher turrets, put moats out in front, bigger drawbridges. And what we didn't really see coming yet is essentially the airplane and the air-to-surface missile."<sup>7</sup> It does not even matter what current threat he was talking about. The same could be said of the floppy viruses of the 1980s<sup>8</sup> and the sophisticated sniffer software found installed at a credit card payment processor in 2009.<sup>9</sup>

There are hundreds of thousands of vulnerabilities out there waiting to be exploited all the time. It is the unforeseen threat that presents a problem. The threat landscape changes constantly as security professionals install preventive measures and criminals need to change their behavior in order to continue to profit from crime. For example, the widespread use of the club that locks steering wheels deterred auto thieves from stealing unattended cars. This phenomenon directly led to the rise in car-jacking, that is, stealing a car by forcing a driver to get out of it. Before the term *car-jacking* was coined, not many people were aware that leaving car doors unlocked while stopped at a traffic light introduced a vulnerability to auto theft. Moreover, unforeseen threats are not necessarily motivated by personal gain on the part of the criminal. Pure vandalism and terrorism is almost always unexpected, as in the example of SHS11.

**SHS11:**

---

One Saturday at 5 a.m. New York time, a user on a personal computer in the Singapore office of a New York-based global firm was browsing the Internet and picked up a previously unknown malicious virus. All PCs in the firm were equipped with anti-virus software, but because the virus was previously unknown, the anti-virus software neither prevented nor detected an infection. The Singapore PC starting connecting over the network to hundreds of desktops in New York. The only detection parameter set on traffic between branches was a bandwidth utilization warning. The single PC did not generate enough traffic to reach utilization levels that would raise the alarm, so no alarms were set off. However, the New York computers soon started contacting each other at the same rate. By 9 a.m., the flood of traffic saturated the processing power of all the workstations in New York. A security guard on patrol through the empty office building heard it first. All the PCs were rebooting. He called the information technology help center. The help center, following procedure, paged the Virus Diagnostic team. A major outage and all-hands-on-deck crisis response was called immediately. An onsite desktop technician immediately isolated a machine displaying the symptoms. He connected its disk to a forensic analysis station in order to safely review its contents. Network analysts identified the traffic patterns and started blocking virus transmissions. Systems engineers researched virus pattern suspects. By the time the desktop technician had the forensics station ready, and network had been stabilized and the engineers were able to talk the technician through isolating the code and delivering it to the anti-virus vendor.

Like SHS9, there was actually no way to prevent the occurrence of SHS11. SHS11 illustrates that it may be the case that detection measures also fail; that is, an asset is damaged and existing detection measures do not detect anything. When this happens, the only way to be secure is to be able to quickly respond to that harm. In this case, the damage was minimal only because the event occurred on a Saturday and because the organization had excellent response procedures in place. Yet, even though the *occurrence* was not preventable, the *damage* was preventable. A post-mortem assessment concluded that there should have been a detection

process, other than an observant physical security guard, for all the desktops in an entire office building being down. Had the machines gone down silently, the event may have been undetected until the users showed up on Monday and tried to turn them back on.

## **MONITOR, MEASURE, MANAGE**

Security reviewers and auditors, depending on their background and experience, may review the facts of SHS11 and recommend a variety of countermeasures to ensure that the threat could not be enacted again. They might, for example, suggest tight restrictions on Internet browsing in the branches, or more alarms on unusual network traffic patterns. However, these recommendations are countermeasures when the situation calls for a holistic view of controls. If a security reviewer were concentrating on the assets at risk in the context of the landscape, it would make more sense to put some kind of detection in place to know whether the personal computers in each office are functioning normally. This type of detection would have set off bells when the first few New York computers started rebooting, and information technology staff would have been alerted hours before the security guard noticed.

An approach to security metrics that monitors assets directly is always superior to an approach that monitors for the single type of threat. It acknowledges that harm in the current business environment cannot be prevented, and the measure will be of immediate usefulness in detecting any event that may bring harm to assets, even if the harm occurs by some other method than that most recently experienced. Therefore, detection of whether computers are functioning normally would be a superior approach to detecting changes in network utilization in response to SHS11 because it is closer to the asset target. However, if there were other assets on the network similarly unprotected, the countermeasure strategy may be a good short-term way to provide coverage for the complete asset landscape against the network-borne threat.

As a management strategy, it is always better to have strong prevention than simple detection. Perhaps one day there will be better prevention for harm to personal computers. But today's situation is that even anti-virus vendors cannot stay abreast of the latest attacks.<sup>10</sup> A CXO must rely on a competent security professional to be aware of general trends and advise on the best combination of prevention, detection, and response process to minimize damage to the asset landscape. With asset harm detection in

place, rather than single event prevention or detection, the information technology staff will be alerted to damage regardless of its cause. Of course, the harm detection should be accompanied by a response process, which in this case should apply to the assets, personal computers. The idea is to get the broadest possible benefit from every security control improvement. Security measures should be evaluated on the extent to which they leave assets vulnerable to threats, but nevertheless should be approached in order to efficiently meet requirements for comprehensive asset protection; countermeasures should be undertaken only as a last resort against immediate threats.

This discussion of alternative security measures in response to SHS11 highlights the fact that security risk management debates are rarely straightforward. Despite the existence of international standards for security risk management,<sup>11</sup> there is so much acknowledged guesswork in every documented approach as to make them all questionable. There will always be multiple alternatives in implementing security controls. One distinguished researcher has gone so far as to say that “Methods for attempting to evaluate security risks are the emperor’s new clothes.”<sup>12</sup> The key is not to be diverted by the question “What’s the risk in not doing anything?” when the security is general in nature and fairly simple to accomplish.

To ensure that an effective Security Program is put into place, a CXO should encourage staff to envision the asset, threat, and vulnerability landscape in a way that facilitates communication and agreement on values with respect to security. For example: “This is the way I see the assets and potential threats. Here is where I think we are vulnerable. I want you to be cognizant of that landscape, anticipate threats I may not have thought about, and in everything you do, make sure you do not create any more vulnerabilities than we already have without involving me in the decision. On the other hand, if you think we need any security measures that affect operations outside of your own department, those should be brought back here for discussion.” When the staff comes back to the CXO’s office with a raging debate on whether some type of security is necessary, this is a red flag that the Security Program itself may need reorganization.

Even in the absence of debate, a CXO should not have to continually make decisions on minute details like the length of passwords or the printing of security badges. Only in cases where the business savvy of the security professional is lacking, as in the example of judgment concerning a recovery point objective, should a CXO expect to get pointed questions on specific business requirements for unique business processes and other assets. If low-level security decisions are often deferred to a CXO, it is an

indication that the Security Program itself is broken. The remediation step in the process cycle of Figure 3-4 has been reached, and it is time to shake up the strategy.

Another indication that the Security Program is not working would be independent evidence that basic requirements are not met. There may be audit findings that assets are missing. There may be evidence in the press that confidential data has been exposed to the public. Customers may report that the integrity or availability of systems or services is poor. A CXO staff may report that requests for security measures are not met on a timely basis. These should all be indicators that the Security Program strategy should be reexamined. Repeated instances of these events should not be referred back to the security department to fix. Assuming the members of the security staff are competent professionals, there is most likely something at the organizational level that needs to be fixed first.



## CHAPTER 4

# SECURE PRODUCTS AND SERVICES

If one considers *weather* a security threat, and this is feasible reasoning in the face of downed power lines due to hurricanes and tornados, one way to secure products is to weatherproof them. The weatherproofing industry has published standards for the level of weather protection that a given coating affords. These standards are clear to all in the industry. They range from fabric threads to electrical connector joints.<sup>1</sup> The analogy with security is that there are commonsense, due care, precautionary measures one should take to protect products, given the set of known hazardous conditions to which they are expected to be exposed.

The production of secure products and services is dependent on the ability to identify threats to the entire lifecycle of the product, not simply upon delivery to the customer. Figure 4-1 illustrates that the product lifecycle chain starts with the supply chain, encompasses the enterprise, and ends only after the customer has thoroughly consumed the product.

### **SPHERE OF CONTROL**

Supply chain threats may affect the product-delivery process, often without the product developer recognizing the damaging impact of the compromised component. The customer experience with the damaged product nevertheless directly reflects on the product developer. Although a component may not

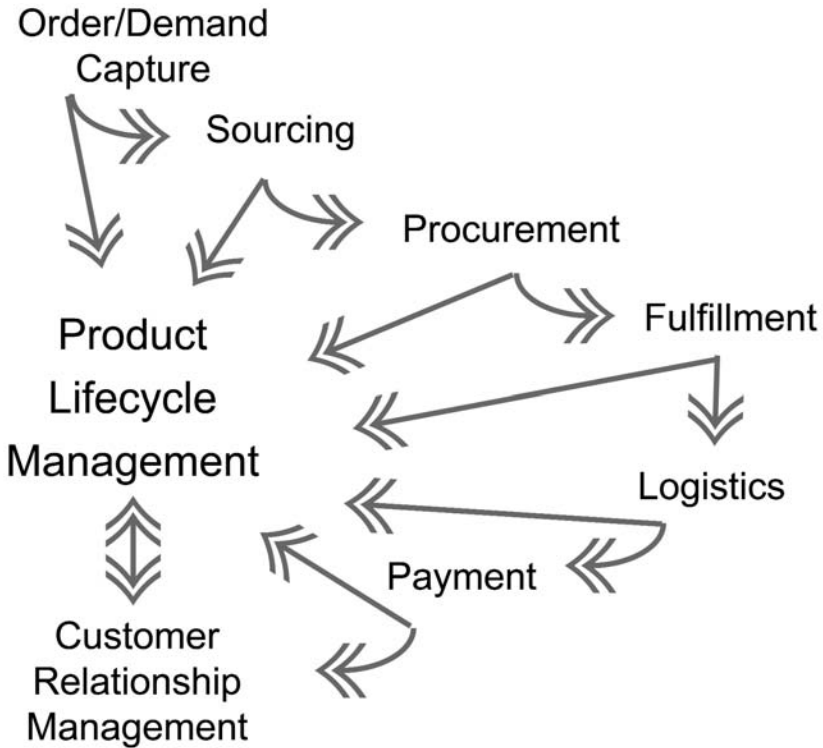


Figure 4-1: Product Lifecycle. Lifecycle components drawn from “The Global Enabled Supply and Demand Chain Map, Version 17,” *Supply and Demand Chain Executive*, Volume 10, Issue 2, 2009.

have been produced within the enterprise, once it is adopted into the business process to deliver a product or service, it becomes an integral part of the product delivered. A CXO can explain the fact that a security issue originated outside of the enterprise business cycle, but is nevertheless faced with a damaged customer relationship. Supply chains are traditionally associated with the manufacturing industry, but any industry that depends on suppliers to deliver products and services is subject to supply chain issues. A common security threat to the supply chain is the proliferation of fake telecommunications parts.<sup>2</sup> As these are incorporated into potentially every industry that uses networks, the fact that the source of the security threat is a manufacturing industry vulnerability has little bearing on the extent of its potential damaging effects.

Post-delivery threats are also closely identified with the product. One of the most famous is the 1982 case in which a few bottles of Tylenol had

been found to be laced with cyanide. The makers of Tylenol voluntarily recalled their entire stock and repackaged their product to include tamper-proof packaging immediately after.<sup>3</sup> That was a superb example of acknowledging and acting on customer security requirements. Moreover, all other major pharmaceutical companies followed suit, making tamper-proof packaging a new industry standard. This is how industry standards get created, though most are nowhere near as quickly publicized and adopted.

There are also cyber security examples of post-delivery threats. At eBay, customers complained that sellers were emailing bidders who had lost an auction after the auction was over, telling the bidder that more product was, in fact, available at a lower price. The bidder would pay for the product and the seller would not ship it. Although the entire fraudulent transaction was performed via email in a method that eBay could not possibly monitor or police, there was so much of this activity that it affected customer perception of the brand. The company made a strategic decision to assist law enforcement in building successful cases against fraudsters, activity that continues to consume a significant amount of time and money.<sup>4</sup>

Note that the examples of reputational damage that happen in the supply chain and post-delivery are not identified as security horror stories. Security horror stories are by definition preventable. Supply chain and post-delivery security incidents are beyond a CXO's ability to control. This calls attention to the fact that no matter how much security one has in place, there will always be some type of event beyond a CXO's ability to ensure threat coverage in a Security Program. However, a CXO can foster the simple recognition that any customer security issue that stems from using a product should be considered a security issue with the product itself. This attitude can put an organization on the right footing to appropriately respond when these events occur. An appropriate response is one that secures the customer relationship.

## **SECURITY VERSUS RISK MANAGEMENT**

One inherent hazardous condition is the sales transaction. No matter what the product or service being sold, there is security vulnerability inherent in the sales transaction. Some sales transaction vulnerabilities are simple to avoid and some are not. Trust is a vital component of the buyer-seller relationship. Product integrity and availability are assumed to be a variable controlled by the seller. Once a product is shipped or a service is

made available, it belongs to the customer. If the product delivery mechanism damages the product, then its security has been tarnished. A package that shows up in tatters on the customer doorstep is not as valuable as it was when it left the factory. From the point of view of the customer, when secure delivery suffers, quality suffers as well. In the cyber security realm as well as the physical security realm, threats to customer delivery are myriad.

## **SHS12:**

---

**Customer Complaint:** “‘I cried for an hour,’ Ms. Gale says. It took a trip to the local computer repair shop and several phone calls with Dell customer-service representatives for her to restore the computer to its factory settings. ‘It was three days of torture.’”

**Facebook’s Response:** “‘Fewer than 1% of Facebook’s 150 million users have become infected with malware using the site,’ says Max Kelly, Facebook’s director of security. “The site started seeing an uptick in malware attacks last summer. . . . Once a compromised account is detected, Facebook will have the account’s passwords reset.”

**MySpace Response:** “Only a ‘negligible amount’ of MySpace’s users have been infected with malware, according to the company.”<sup>5</sup>

**U.S. Military Response:** “These Internet sites in general are a proven haven for malicious actors and content and are particularly high risk due to information exposure, user-generated content and targeting by adversaries.”<sup>6</sup>

The message to the affected customer is clear. Rather than being built into the product, security is an afterthought. The company is comfortable if some low priority customers have to put up with occasional pain as long as the company continues to make money in aggregate. Unfortunately, this is the approach taken by CXOs too often. Rather than face the security threat head-on, they take comfort in risk management calculation and remediation measures. They acknowledge individual customer suffering as long as it does not affect the bottom line.

A principle from the world of medicine is applicable here. First, do no harm. A company that has a Web site that carries malicious programs disguised as advertising, like the one in SHS9, is a danger to its customers.

There are a growing number of security horror stories that indicate regulators and courts would agree. SHS13 describes a case against a company that had a privacy policy posted on its Web site that deceived customers about the level of security that could be expected in the product.

**SHS13:**

---

“Companies either did not encrypt consumer information in their database, or encrypted using a nonstandard proprietary system with significant weaknesses, leaving the data vulnerable to commonly known and reasonably foreseeable attacks from third parties. The commission alleged that the advertisers had committed deceptive acts by falsely claiming that their security practices were consistent with industry standards. The FTC (US Federal Trade Commission) also claimed that the companies had committed deceptive acts by failing to use reasonable and appropriate means to protect consumer data against unauthorized access as they had promised, instead leaving the data open to attack. ValueClick agreed to pay a record . . .”<sup>7</sup>

Even in cases where no claim to provide security is made, regulators and courts are now fully aware of the fact that companies should be held accountable for providing adequate security. In the United States, the Federal Trade Commission has repeatedly established that inadequate security is an unfair business practice, as in SHS14.

**SHS14:**

---

“The FTC claimed that BJ’s Wholesale did not take reasonable and appropriate measures to protect (customer) information in their computer systems, and it was accessed and used by unauthorized individuals to make about \$13 million in fraudulent purchases. The FTC alleged that BJ’s Wholesale’s failure to adequately protect consumer information was an unfair act or practice.”<sup>8</sup>

SHS13 and SHS14 happen to be U.S. FTC cases, but the scope of legal obligations to provide security has become global.<sup>9</sup> The moral of these

cases is that a CXO should do everything within power to avoid victimizing customers. Don't assume that a product has to inflict damage firsthand in order to harm customers. Customers can be harmed indirectly if a company's services are exposed to fraud. If it is easy for a fraudster to steal a customer's rights to a product, then the customer is exposed to damage in the course of the purchase. In theory, it sounds self-destructive for any business to do this. In practice, it is being done every day. Every time someone uses a credit card number that does not belong to them, the bank becomes a fraud enabler.

One explanation is that it is usually not security management personnel, but risk management professionals that make decisions about just what level of insecurity a product line will bear. Risk management practices are designed to protect an institution, not its customers. When U.S. regulators required banking institutions to adopt a measure to place a \$50 lid on the amount a customer has to pay on a reported credit card fraud, banks deemed the cost of compensating the victimized customers a price small to pay compared to mounting an all-out effort to prevent credit card fraud.<sup>10</sup> The \$50 limit on personal harm may have stopped customers from worrying about credit card fraud, but it has not prevented customers who experience it from losing faith in their banking institution. The risk managers who adopted the approach used a tactical, short-term solution when a longer-term, customer security strategy was required to combat the now rapidly escalating globally organized crime of systematic identity theft.

Even in cases where the risk managers prevail, and some level of vulnerability may be tolerable, a CXO should not dismiss threats for which some protection exists. The risk may be acceptable now, but like the \$50 lid on credit card theft, it might not be acceptable going forward. There is a difference between *risk tolerance* and *risk acceptance*. Risk tolerance, sometimes referred to by risk professionals as *risk appetite*, implies that there is a situation in which the business impact from a threat is so minimal that it does not have to be addressed.<sup>11</sup> Risk acceptance, on the other hand, implies that there is business impact expected from a threat, but it has been decided that the probability of the threat being enacted is too low to bother to mitigate the associated vulnerability. If an organization has an appetite for risk, one will sometimes find the risk acceptance professionals using lower likelihood and loss expectancy estimates for business impacting events. This may lead to acceptance of vulnerabilities that are easily corrected.

Note that financial calculations with respect to business impact of fraudulent credit-related security issues are not isolated to the financial industry. Other companies have similar exposures. Every time someone uses a calling-card number or a shipping number that does not belong to them, the real account-holder is compromised. When products change hands from the provider to the fraudster, the real customer of the provider is charged. The burden is placed on the customer to detect and report the event. Every CXO should be alert for scenarios where such an event may occur on their watch.

One such scenario occurs when a company Web site is compromised and loaded with malicious software, known as *malware*. Where malware is traced and reported to authorities, the company that is hosting it may end up on some security watchdog's list of disreputable sites.<sup>12</sup> The watchdogs distribute their lists to security service providers, with the consequence that any site on the list will be immediately blocked by a wide variety of security mechanisms that subscribe to the list. A company that gets on one of these lists by mistake may find that customers are prevented from getting to their Web site for their own good, and it can take days to prove to the watchdogs that the malware has been eliminated. For this reason alone, preventing customer damage due to malware should be a core competency for any reasonably robust baseline security program. It should not slip to the side where risk managers start debating whether or not it is OK to be hosting malware. To entertain the debate on whether a company should control the software that people run from its own Web site is to invite damage to its brand.

## THE CLIENT PERSPECTIVE

In 2000, a renowned security professional wrote, "I'm continually amazed by the number of commercial security systems with gaping holes that the designer never noticed, because they spent all their efforts securing pieces they understood well."<sup>13</sup> The situation has not changed. That is, a company may design a security product or service to meet one security requirement, and sell it to someone who needs to meet the security requirement. But if the designer does not consider the asset landscape of which they would become a part, then once the product or service is deployed within the enterprise, the enterprise may be less secure overall than before it was installed. An easily understood example is found in SHS15.

**SHS15:**

---

A company hosts emergency contact sites. These are Internet web applications that allow a security manager to enter the home phone numbers, cell phone numbers, and private email addresses of the company's senior executives and security emergency response team. The sites also allow the manager to enter a message that will be simultaneously sent to the people on the list via automated voice mails and emails. A physical security group had a great need for such a system to communicate with executive management in the event of an emergency. As it was a decision to outsource an IT function, the system was required to undergo a due-diligence security review, a task which fell to the information security group. The information security group found that the site developers did not follow software industry standard secure architecture or coding practices. So, theoretically, the personal contact information for the entire executive management and security teams would be exposed to potential Internet hacking attempts. Successful hackers would also have the ability to send these teams messages that would appear to them to be an emergency notification to and from the executive management.

The fact that an otherwise sincere security vendor often leaves customers exposed is due to a fundamental lack of understanding with respect to the threat landscape. It reflects a phenomenon long known to security professionals, and recently coined as “the attacker’s advantage and the defender’s dilemma.”<sup>14</sup> No single security feature can secure an asset in isolation. Security results only from a combination of people, process and technology that together provide prevention, detection, and response mechanisms at the asset periphery. Security professionals must constantly defend all known accessible points on that periphery, but attackers can scan at their leisure for possible new avenues of entry and opportunistically choose the weakest one they can find.

A CXO should encourage security staff to constantly reevaluate the threat landscape from the perspective of the customer. When it comes to customer perception of the security of a product, the worst security horror stories are the ones the company never knew happened.



**SHS16:**

---

A salesperson from an online information technology service company was courting a potentially very big client. The system he was selling allowed clients to enter information about products, prices, and customers. It had all the accounting, billing, and reporting features necessary to run a business. Clients could add users, and designate who could read and update data on a screen by screen basis. The potential client seemed sold on the system, but wanted to send a group of technical people to ask some questions about how the system worked. The salesperson arranged a meeting between his own technical staff and that of the potential client. The two teams hovered around a single screen as the online company's technicians displayed screen after screen to the prospect's technicians. A member of the prospect team asked, "How do you protect our data in your system from being seen by your other clients?" The technician responded that there was no screen by which this part of the system security was exposed, but volunteered to show them anyway. He clicked away until all could see he was at a text-based computer prompt usually not seen by clients. He demonstrated that each client was allocated a separate database file. The prospect team then asked, "Who can access these database files like you just did?" The technician did not know the answer right away, but entered a command that he knew would list the users who had permission to view the database files. The list only had one entry: "Everyone." The technician explained that this did not mean all Internet users, or even all clients, but that in this case, "Everyone" meant just all users that had access to the low-level system functions, which meant only the people that worked for the online company. But it was too late. The technical team from the potential client was appalled at the low level of security and recommended against the online system. The salesperson was told simply that his competitors had superior technical solutions. The technician who did the demo did not consider the event significant enough to report.

This type of security horror story is quite common. Engineers and technicians assigned to sales duty are conditioned to highlight the advantages of their products and gloss over disadvantages. When a current and/or a

potential client insists on a security feature that is not in the current product, they are usually told that there are dozens of clients happily using the product without the requested level of security.

Cases like SHS16 tend to occur more on the logical side of security. It is sometimes hard for information security professionals to communicate to product designers that not all logical security features are created equal. Too often, security measures are designed at very superficial points within a computer system, with the result that data is left exposed. Access to data is facilitated through networks and screens in such quick and creative ways that mechanisms for data security are left out. Vendors often take the easy way out and make superficial use of security logins or restrictions designed for some other data delivery process. It is a constant concern to security professionals that systems are programmed to hide data from users instead of to secure it properly. Users think the data is secure, but unauthorized access can be had by highly technical individuals who know the right commands. Security professionals have coined the term *security through obscurity* to refer to this phenomenon.

Even when there is some real login security, groups of users are often given similar permissions to data in order to make an administration process easier to manage. This may be true even if some group members see the data through screens that seem to restrict their access. In the latter case, security through obscurity prevents most group members from knowing how much access they really have (most, but not all, because the technical ones know how to exploit these vulnerabilities).

Security architects and reviewers who deal frequently with vendor selection are repeatedly challenged on whether the security features are important enough to the business to make or break the sale. Even vendors who include security as part of their marketing program sometimes fail to understand that there must be substance underneath the marketing claim in order to actually meet customer expectations. Nowhere is security theater as rampant as it is in the course of exercises in “vendor due diligence.” If a company participates in any sort of outsourcing arrangement whereby a third party is exposed to information that is under regulatory scrutiny, the company is not relieved of its own regulatory requirements with respect to the security of the information, so it must perform “due diligence” to ensure that the vendor safeguards the information before commencing the outsourcing arrangement. Firms are also required to periodically (commonly construed to mean annually) repeat due diligence thereafter.

So many security professionals turn this “due diligence” part of their job into an easy and boring checklist exercise (with occasional travel) that outsourcing vendors find ways to make it entertaining. This is illustrated in SHS17.

**SHS17:**

---

“I was on a site evaluation team visiting a data center at a hosting service provider. Upon arrival, we stood in a conference room with our vendor sales exec, the head of operations at the center, and some of his high level managers. They told us what we would be seeing on our tour. They described a state-of-the-art network, enormous storage capacity, caged servers with biometric security devices, and service levels that were supported by highly skilled technicians. At the end of this impressive overview, triumphant music filled the air and a previously inconspicuous curtain on the wall behind us parted to reveal a balcony view of the network operations center. There were wall-to-wall screens with graphics depicting network routes, utilization statistics, and red/yellow/green alerts. There were clusters of workstations in tiered semicircles facing the big screens, each with a sign hanging from the ceiling to identify its purpose. Server operations, network operations, data administration, performance monitoring, job control, and others. We stared quietly as the vendor staff beamed on the display.

My stare was in disbelief, first at the scene, then at the beaming staff, and then back. The cluster of workstations labeled ‘security operations’ was empty. The screens showed red alarms and there was no one sitting in front of them. No one else noticed.

I had to mention it: ‘Why is there no one at the security station?’ I asked. The sales exec looks at the head of operations, who looks at his staff, who look at each other. One of them finally stepped forward. ‘Administrators play multiple roles,’ he said, ‘and they stand up and walk around to man different workstations as tasks are necessary to be done in other areas.’ Well, this didn’t ease my concern. ‘So then,’ I pressed, ‘who is logged in to each workstation, and how do you maintain accountability for administrative activities where people are sharing terminals?’

The staff again exchanged looks before one answered the question. ‘They cannot really do much from these workstations; they are mostly used for monitoring.’ He said it with a finality that considered the subject closed. He smiled and led the gathering to the other side of the room to discuss the day’s schedule. His attitude had quickly shifted from, ‘see how great our operations center looks’ to ‘pay no attention to the men behind the curtain.’”<sup>15</sup>

The portrayal of security requirements as minimal persists even in the presence of large communities of security reviewers simultaneously being told by the same vendor that no other firm needs the level of security that is expected. Only after experiencing a security horror story do such vendors voluntarily include security into their products and services.

This situation recalls the bridge analogy of Chapter 2. It is like a mayor of a small town negotiating with a bridge builder and the builder saying, “but no other communities care if their bridge has structural flaws.” It is hard to imagine circumstances where a mayor should be assured by that argument. A CXO should understand the extent to which business process relies on key infrastructure and people in the asset landscape, and instinctively recoil from circumstances in which those assets are poorly preserved. The reliance on that business process, and corresponding assets, to maintain an ongoing concern includes reliance on service provider and supplier safety and security. An organization’s institutional knowledge should encompass an in-depth, shared understanding of business process that includes the customer.

For example, consider an online service provider that markets information processing services to business customers like the one in SHS16. Say they operate in an industry wherein all the online service users always work in the customer’s offices. In this scenario, a commonly requested security feature is to restrict Internet access to customer data to computers residing in the customer’s offices.<sup>16</sup> It is obvious to all customer security reviewers that this feature is desirable from a security standpoint, yet each security reviewer is told by the service provider that no other customer security staff has a requirement for it. An extreme case of ignoring obvious customer security requirements is described in SHS18.

**SHS18:**

---

“Cyberspies have penetrated the U.S. electrical grid . . . said a former Department of Homeland Security official. ‘There are intrusions, and they are growing,’ the former official said, referring to electrical systems . . . Authorities investigating the intrusions have found software tools left behind that could be used to destroy infrastructure components, the senior intelligence official said. He added, ‘If we go to war with them, they will try to turn them on.’

“Last year, a senior Central Intelligence Agency official, Tom Donahue, told a meeting of utility company representatives in New Orleans that a cyberattack had taken out power equipment in multiple regions outside the U.S. The outage was followed with extortion demands, he said.”<sup>17</sup>

The fact that these intrusions have been the subject of regulatory scrutiny for years means that power companies are engineered in such a way that they are hesitant to disconnect the network that controls the U.S. power grid from the Internet. Such completely sloppy perimeters in network security are an extreme example of complete disregard for customer security in favor of some internal expediency goal. Internet attacks were a well understood threat long before the power companies ever became dependent on the Internet. The entire situation was completely avoidable and yet an energy industry spokesperson has been quoted as saying, “We can have a bulletproof system and absolutely no one could afford the electricity.”<sup>18</sup> The consumer is asked to believe that private telecommunications lines are beyond the energy industry’s ability to afford.

## **PATTERN RECOGNITION**

A CXO should not be lulled by the fact that fraud events are industry-wide problems or that exploits of vulnerabilities are few and far between. A CXO should instead concentrate on how vulnerable the assets are, and remember that the unexpected threat is the one that may do the most amount of damage. SHS19 illustrates this point.

### **SHS19:**

---

“Overseas hackers broke into customer accounts at two popular online stock brokerages, TD Ameritrade Holding Corp. and E-Trade Financial Corp., in a ‘pump and dump’ stock-trading scheme that led to at least \$22 million in losses.

The attacks, which took place during the last three months, were launched by identity thieves in Eastern Europe and Asia who primarily used keylogging software delivered via Trojan horses or other

malware to steal users' confidential information as they logged onto public computers or their own infected machines, TD Ameritrade CIO Jerry Bartlett said in an interview today.

The hackers then logged into existing customer accounts-or created dummy accounts-to buy shares in little-traded stocks, driving prices up so they could sell their own previously purchased shares for a profit.

TD Ameritrade said in its investor conference call today that it had spent \$4 million to compensate customers who suffered losses after their accounts were broken into.

E-Trade confirmed in an investor conference call on Oct. 18 that it had spent \$18 million to compensate customers. CEO Mitchell Caplan told investors that E-Trade has cut its losses to 'almost zero' in the past three weeks after beefing up its security."<sup>19</sup>

The preventable aspect of this security horror story is included in the text. Once the company decided that it needed to "beef up" security to prevent further exploits, the fraud disappeared. The story does not include the fact that when the incident was first detected, losses were much lower, and the recognition that the fraud was rapidly accelerating came too late to prevent huge losses and untold customer anguish. Had the company been quicker to react, both the escalating cost and the customer confidence damage over a several-month time period could have been minimized. It is OK to be the first to discover a vulnerability that affects customers, but prompt response to a known threat is essential to keeping their trust.

What is important to note about these industry standard due care measures is that everyone knows what they are; no matter how arcane a security horror story appears to a business, the customers usually see it in much more simple black-and-white terms. The comedian Lewis Black gives us an example of this in SHS20.

### **SHS20:**

---

Black starts with a plea for proactive customer service. "If you know something is going to go wrong, and you know why something is going to go wrong, and you have already experienced the pain and trauma of it going wrong, wouldn't you make a profoundly con-

certed effort to avoid it happening again?” He tells the story of a seemingly endless wait for a flight, which the airline blamed on a system-wide computer glitch. In colorful and entertaining language, he emphasizes that any intelligent person, in this day and age, needs only common sense to understand that computer glitches can be planned for and avoided with redundancy measures. Black closes the story with, “It’s like inventing fire, and not keeping something lit, in case the main fire goes out. If our ancestors were as dumb as we are, we wouldn’t be here.”<sup>20</sup>

The moral of SHS20 is that, if a *Comedy Central* comedian can claim to a mainstream audience that it is obvious there are no security controls in place, then it will be extremely difficult to explain to customers why security was not considered when designing their product or service. Good security is like continuous performance of a traditional telephone line. It is taken for granted while the phone is working, and once it goes off, there is no memory of how long it was working without interruption. The difference between good security and bad security is that, in the latter case, you were only keeping your friends out and they resent the inconvenience.

Without a comprehensive organizational approach to security, a CXO cannot expect that even post-SHS measures will be based on any other principal. Nevertheless, it is so common a tendency among CXOs to believe that security horror stories cannot happen to them that security professionals have a phrase for it: *Depth-of-Denial*.<sup>21</sup> The phrase is used to refer to a CXO who believes that it is possible to maintain plausible deniability that there are any vulnerabilities in the asset landscape. The word *depth* refers to the low probability that the denial is justified. A CXO in denial may claim that they are in the same situation as was their last company, or competitor, or some other reference to someone else who does not deal well with vulnerabilities. It used to be that the worst fate that could befall a security professional due to a security horror story was that their misery may be reported on the front page of the *Wall Street Journal*.<sup>22</sup> It is now that their CXO may end up being quoted on *The Daily Show with Jon Stewart*.

*This page intentionally left blank*



## CHAPTER 5

# SECURITY THROUGH MATRIX MANAGEMENT

Vertical solid lines in an organization chart typically represent that the person higher on the chart directly manages the work of the person lower on the chart. Dotted or dashed lines in an organization chart typically mean that the person on one end of the line has some kind of responsibility for work done by the person at the other end, or vice versa, or both; but there is no direct reporting relationship. Whether or not dotted or dashed lines are formally represented on an organization chart, security roles and responsibilities often follow the dotted line, or *matrix management*, model. A comprehensive Security Program is rarely managed fully within every department accountable for securing assets. CXOs of all departments that handle assets should get some direction from, and provide feedback to, the Security Program.

There are as many ways to organize security as there are organizational structures. If the CXOs in a given organization are a tight-knit group, accustomed to close coordination, then it should not matter to which CXO the person(s) managing the Security Program reports. If the CXOs are not a tight group, then either there will be multiple Security Programs, or the Security Program may end up too far below C-level to be effective for organizations other than that of the CXO to which it reports. Even if CXOs generally work well together toward common goals, if there are multiple Security Programs that are not connected via an

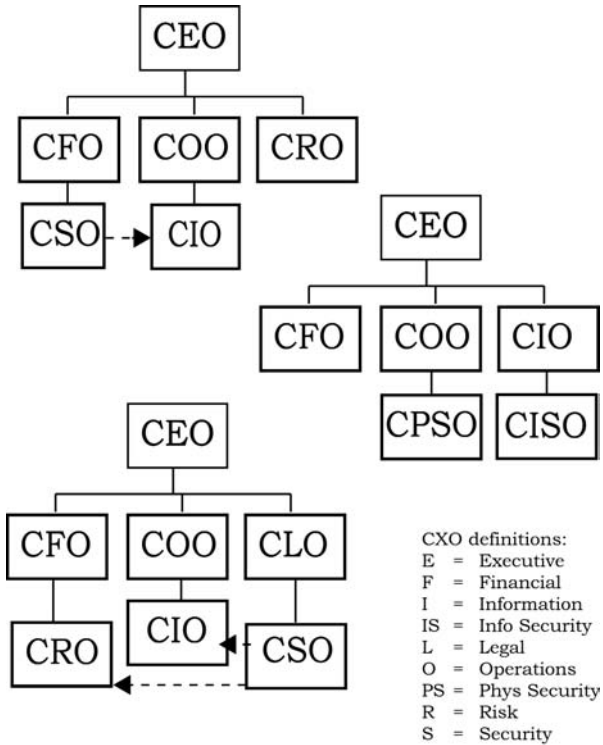


Figure 5-1: Alternative Organizational Structures

explicit organizational strategy, then the uncoordinated work is likely to result in either unexpected gaps or overlaps in general controls. The former would lurk between the seams of the organization; the latter would preclude economies of scale.

Figure 5-1 presents several alternative reporting structures that are in place in different large organizations. Some of the most heated debates among security professionals in the past few years have been on the topic of where security should report. The debates have ended in a stalemate. Because the placement of the security organization itself deeply influences the objectives of the Security Program, it is almost impossible to make a comparison between the alternatives. Where security reports to a legal function, its primary objective tends to be regulatory and contractual compliance. Where it reports to a financial function, its primary objective tends to be asset protection. Where it reports to an operations function, its primary objective tends to be resiliency.

## ISSUES WITH DATA

Unfortunately, the field of security metrics is too immature to provide any direct evidence that one organizational structure works any better than any other.<sup>1</sup> A unified Security Program that completely covers all security requirements can only be accomplished in the context of an integrated approach to security at the CXO level. Nevertheless, there is a requirement that some manager, presumably the highest ranking person whose sole responsibility is security, understands the integration well enough to know what each organization is measuring to validate compliance with holistic security objectives. Even if the security metrics function is split across multiple organizations, there should be some check and balance to ensure that all the organizations are singing from the same page. In security terms, this means that all organizations who refer to the same assets or controls in their metrics agree on what information should be available in order to fully describe those assets and that data with respect to those definitions has integrity.

This may seem like an obvious example, but suppose a physical security group is tasked with handing out physical security badges and a logical security group is tasked with handing out computer passwords. Say a department hires a new individual who needs both physical and logical access. The department should only have to notify one group that a new person has arrived. That group should maintain a master list of authorized users of firm resources. The first and last name of the individual should never be entered twice. In this case, security responsibility for this master list typically belongs neither to the physical or logical security group, but is trusted to the human resources department. The list maintained by the human resources department should then become the baseline by which all other access is measured. If the physical security metrics and the logical security metrics have any numbers that are percentages of the total set of potentially active resource users, the 100 percent number should be the same in both places, and it should match the total number in the list maintained by human resources. Where individuals on the list are directly identified in investigations, the first and last name should be spelled the same by both departments, and that spelling should come from human resources.

The example seems obvious because any CXO will intuitively understand counting people. However, there are many aspects of the asset landscape that are more difficult to map onto baseline data repositories. SHS21 provides an example.

**SHS21:**

---

A dangerous new Internet virus was announced to be active on the Internet. There was a fix, or a patch, available that, if installed on a PC, would prevent the virus from harming the PC. Using a network scanner, the logical security group identified ~3,000 machines on the network that were vulnerable to the new virus. They notified the desktop support group that the machines on their list should be patched immediately. The desktop support group had an automated patch delivery system that was integrated with an inventory database of over 4,000 machines. The manager of the desktop support group thought it would be easier and safer to apply the patch to all the machines in inventory, instead of just the 3,000 known to be vulnerable. The security group agreed with the approach.

The day after the patch was installed, several users complained that their PCs were unusually slow to the point of being unusable. The machines were found to be infected with the new virus. They were also on the logical security group's list of vulnerable machines. Upon investigation, it was discovered that the infected machines were missing from the desktop support group's inventory database.

**ISSUES WITH LEADERSHIP**

An integrated approach to security organization and metrics does not imply that everyone working in security has to take orders from a central authority. Rather, it implies only that business objectives for security are agreed upon and that roles and responsibilities for security measures and baseline inventories have been delegated to the organization best suited to assume them. An integrated approach to security may even allow for fully functional security departments to report to different CXOs, as long as their activities are actively coordinated to ensure that economies of scale are achieved without business requirements getting lost. However, the integration cannot be left to security staff. It must be devised at the CXO level in order to be effective. Organization structures in themselves can generate security horror stories.

**SHS22:**

---

A large organization was plagued by negative, information security–related audit findings. It seemed no matter how much money the technology departments spent on security, the findings were always there. The CIOs got together and decided to pool their resources. All of the information security staff was centralized under one of them.

The volunteer CIO hired a very high level and expensive security officer to organize this central group to make it efficient and effective. The person divided the security staff into departments, each concentrating on a distinct aspect of information security. One group was dedicated to general controls, another to policy, and others to risk assessment within the business areas. Results of the risk assessments were provided directly to the technology staff in the business area for risk mitigation. A set of application systems that allowed standard documentation with respect to risk assessment was devised, and so a security software development group was also formed to provide software for the security management effort.

After two years of this approach, the audit findings were still there. The CIOs in the other business areas had ceased to be concerned with security as soon as the staff was transferred out of their control. As there was no tone at the top, the various technologists in the business areas plagued by audit findings were not motivated to respond to risk assessments. Instead, they complained it was a mistake to create the central organization, which had created a drain on resources without fulfilling its mission. The new risk assessment repository started piling up with documented security risks, and this became another audit finding.

The CIO to which the security officer reported directed the security officer to divide the security risk assessment teams up in such a way that they could be transferred back into the business area. The general controls, the software group, and the policy group were kept central. The security officer still claimed efficiency by requiring the distributed risk assessment groups to follow the centrally devised processes. However, as soon as the business security groups got back

to their own business areas, the CIOs to whom they reported directed them to address the problems and issues within the CIO organization. They found that the centralized methodologies did not map to the problems they faced and adopted new approaches. As the central group no longer had any responsibility for the business area activities, they did not attempt to enforce policy, but simply recorded what the business areas were doing, which was mostly not following the central security process.

Audit continued to deal with the central security group as their main point of contact. The negative audit findings, of course, persisted.

SHS22 is an example of a “separatist” approach to security management. On paper, it looks like matrix management (see Figure 5-2). But it does not actually *manage* those at the other end of its dotted lines; it simply informs them and reports on them. A separatist central group is entirely hands-off. It is intended to work by influence, but in fact provides little in the way of actual control points. CXOs who fund such groups should be aware that they provide about as much security as an external best practice organization combined with internal audit. Often, the “influenced” organizations see the separatist group as either a disconnected dictator of the impossible, or, at the other extreme, a convenient source for a security requirements checklist that relieves them of responsibility for anything except what is on the checklist.

The failure of the separatist approach stems from the fact that it leaves an accountability gap between those deciding what should be done, and those understanding the day-to-day issues faced by the organization. The central security group is expected to be omniscient when it comes to requirements, while the business areas handle the assets. Often the central group, recognizing that they are not actually omniscient, will give security staff in the business areas leeway to ignore policy that does not make sense. But the business areas don’t substitute the senseless policy with a commonsense one, as policy making is not their function.

Where a separatist central group is charged with oversight as well as policy, they create and execute programs that look very much like internal audits. As most organizations that try this approach are of a size to have an internal audit team as well, it makes the audit job function with respect to security almost superfluous. Moreover, the existence of the oversight function creates the *impression* that security is managed centrally when it actually is not. The real internal auditors tend to discuss systemic security

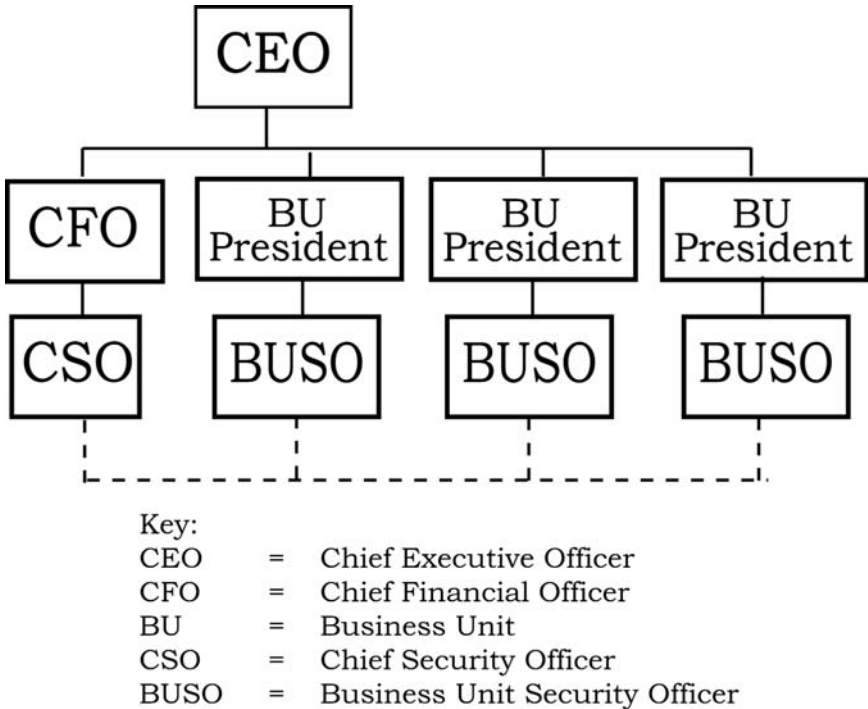


Figure 5-2: Example Separatist Organizational Structures

problems with the central security group, with the consequence that all business oversight of the security function is left to people whose main job has very little to do with running the business.

While a CXO may experience a rise in security levels soon after appointing a separatist central security group, that short-term spike is often simply due to the tone at the top it took for the CXO to create the central group. Where a new group is charged with writing policy, there may be an initial attempt to comply. But if the group is given no management tentacles into the organizations that actually control assets on a day-to-day basis, staff will quickly realize that there are no consequences for not following policy, and policy compliance will not be anyone's priority. Where organizations have a history of general apathy toward security, the central group quickly becomes another example of inefficient and ineffective security theater. At worst, the creation of a separatist security group sends a message to staff at the operations level that they are no longer responsible for security. They stop doing it, although there is nothing at the operations level to take its place.

To give credit to the CIOs facing a hard problem in SHS22, a coordinated approach to security is definitely the right track. CXOs often see a central security group as the only solution to a resource issue. That is, they want to separate some resources who know what should be done from the people who are torn on a day-to-day basis between what needs to be done for security and other things they need to do as part of their jobs. A central security group is not always as ineffective as that in SHS22. It is only where the central group has no responsibility for results that it is destined to fail.

## FOCUS ON COORDINATION

A central security group that is hands-on and accountable at the organization-wide level has a chance at succeeding. A central security process can work with business areas to identify and dictate actual security measures with or without writing policy or supervising implementation. They can coordinate security activities by leveraging business processes that are used to handle assets, and designing control points within it. Where it is generally understood how the Security Program is supposed to work via a matrix management approach, processes that provide security will be obvious throughout the organization, and they will be enforced at all levels of management.

For example, take the situation faced in SHS10, the one in which multiple branches maintained their own payroll and procedures for personnel access control. Under the separatist approach, the solution would be for a central organization to establish a policy that *each branch shall have a process by which authoritative personnel lists were kept up to date, and access control shall be configured only for currently active personnel*. Each branch would individually produce procedures to do just that. The central security group would then audit each branch. The central security group would first have to review the branch's procedures to make sure control points were adequate, and then verify that they were done correctly. In some cases, the central security group might simply seek formal confirmation by some branch manager that procedures were in place rather than performing an actual verification. Of course, there would be staff and access control processes in the central organization as well, so some security staff would have to be charged with creating procedures for the central entity as well.

By contrast, a *coordinated* central approach to the solution for SHS10 would be to first gain agreement on a business goal stating that the manner by which all employee payroll and non-employee staff authorization records were created, archived, and stored would be centrally devised in cooperation





Figure 5-3: Example Matrix Organization

with the business areas. A process whereby the records are used to configure, or to audit the configuration of, access control systems would be universally agreed. Each CXO would endorse the business goal and participate in the process, and internal audit would be catching mistakes in process implementation in all business areas. It is obvious that the latter (coordinated) approach is more efficient and effective than the former (separatist) approach. The documented policy would be the same in either case.

The key to success in a coordinated Security Program is to form cooperative teams among like job functions in disparate business areas. Not security job functions, but job functions of those handling assets. A Security Program should be able to harness the collective intelligence of those in the same job function across multiple organizations and get them to propose and agree upon a “right way” for an organization to achieve its security goals. This is a quintessential example of the conditions under which matrix management makes sense. As illustrated in Figure 5-3, a

Security Program's matrix organization chart often has numerous dimensions. It will include a variety of cross-organizational teams and dotted line reporting functions. With very little in the way of direct line reporting, it will encompass virtually every area of the organizational structure.

Of course, an organization that has a comprehensive and pervasive Security Program in place will only be as secure as the results it produces. It will produce good results only if people who are recruited to be on cross-organizational teams take their role in the Security Program seriously. Even where CXO objectives for security are codified in documented policy, it may nevertheless be hard to get people who are focused on a specific low-level business deliverable to productively participate in a Security Program. This is where tone at the top comes in. There must be no excuse.

Cooperating with a Security Program must be seen as something that allows a job to be done smarter. Learning about security must be perceived as a resume-enhancement. As with tone at the top, these perceptions can only be achieved via the same mechanisms that job satisfaction is achieved generally, with feedback related to job performance. For example, one way to do this is by tying some percentage of a person's bonus to adequate performance in the security spectrum. Whatever the method, it has to be visible and in conformance with the method by which employee recognition is generally achieved.

Detractors of the coordinated approach to security often complain that their organizations lack the skill sets and resources required to secure assets. Unfortunately, that argument is universal. There is not enough subject matter expertise in the world even to perform regulatory required security audits, much less implement all the security that can reasonably be done to keep critical infrastructure safe.<sup>2</sup> The best response to this argument is to counter that it is the CXO security strategy to bring all lagging organizations up to speed, that dedicated security personnel do not bring in profits, and that every manager will be judged on their organization's ability to perform the expected security role. It is also helpful to ensure that the Security Program includes documentation that clearly outlines each role, along with the applicable security responsibilities, as in the example of Table 5-1. Where the role is clear, corresponding training programs may be devised to bring those who find themselves in the role up to speed on the security capability demanded by it.

The idea that multiple organizations may be charged with security and still produce a coordinated Security Program is a topic of debate among security professionals. A substantial body of literature has appeared under the topic of *convergence*.<sup>3</sup> By convergence, security professionals mean the

**Table 5-1**  
**Roles and Responsibilities**

Role	Security Responsibility
Business Process Directors	<p>Information is classified as intellectual property, business proprietary, client-related, or public.</p> <p>Access to both physical and logical assets is granted such that it is the minimum required by an individual's current job function.</p> <p>Security requirements are included in business planning, and control measures are tested prior to being implemented.</p> <p>All system changes are documented and reviewed by a change review board.</p> <p>Users are trained on new applications and new security features of applications prior to each production implementation.</p>
Real Estate Management	<p>Physical security is monitored via cameras in areas where assets are portable. Camera replay of incidents are tested and meet service levels required for prompt investigation.</p> <p>Physical security access logs are archived in such a way that reports of individual activity may be quickly retrieved in the event they are needed for an investigation.</p> <p>Physical security is maintained via centrally controlled badge access, and departments are trained on badge distribution and termination procedures.</p> <p>Environmental controls are designed to ensure that electronic equipment may continuously operate within guidelines for acceptable temperature, power, and humidity levels.</p> <p>Paper is physically secured and discarded in a form that cannot be read or reconstructed.</p>
Human Resources	<p>Security roles and responsibilities are assigned to every individual via job function. Policy and procedure enforces accountability for compliance with security policy; consequences for non-compliance include dismissal.</p> <p>All employee and non-employee staff are educated on information security responsibilities as part of orientation. They must sign that they have read and understood a Security Responsibilities Statement.</p> <p>All individuals who perform work onsite are screened to ensure there is no background of criminal activity or indicators of fraud.</p>

**Table 5-1 (continued)**

---

	<p>A list of active employees and non-employee workers has unique identifiers for each individual and current department and job function.</p>
Lawyers	<p>Asset protection requirements are included in contracts with third parties handling assets held off site and enforced for those who are onsite.</p> <p>Regulations that apply to the business and require the incorporation of security controls in order to meet regulatory requirements are identified and digested into Security Program requirements.</p>
Technology Directors	<p>Information technology personnel are empowered to enforce security policy compliance.</p> <p>Similar data of the same classification level is stored according to business security requirements consistently across business applications.</p> <p>Systems inventory is maintained at the business processes level. Firmwide data flow identifies security control points.</p> <p>Technology infrastructure is architected to be readily available during global business hours. System maintenance is planned in order to avoid service interruption.</p> <p>Standards for interoperability, performance, efficiency, and scalability are enforced.</p> <p>The network restricts Web access to sites that are identified as non-business related.</p>
Accountants	<p>Approved data flow from business process and information systems to financial statement generation is documented and maintained.</p> <p>Identify control points to detect inconsistencies in data entry, reconciliations, and account balances that are common targets of financial fraud or asset theft.</p>
ProcurementManagers	<p>Establish and maintain procedures to correlate business requirements with procurement efforts. Ensure that multiple vendor bids are solicited for commodity products and services.</p> <p>All vendors that handle information assets are tracked by BU, contact, vendor type and function, and connectivity. Vendors who use data off site must periodically demonstrate due diligence in data handling commensurate with risk of data leakage or loss.</p>

---

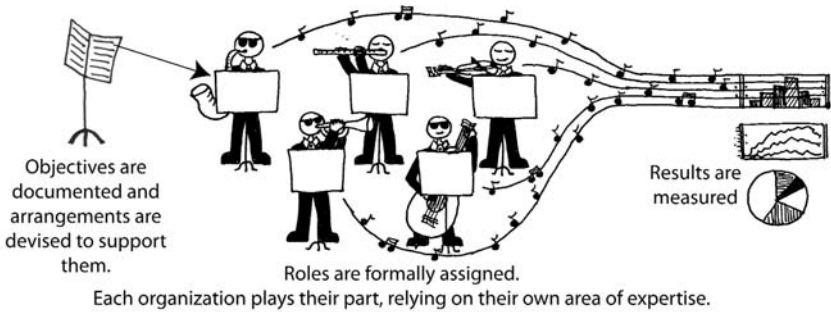


Figure 5-4: Accountability Flow

expectation that physical and logical security practitioners will generate integrated and cross-functional solutions to business security problems. The convergence literature often exhorts CXOs to merge their physical and logical security organizations in order to jump-start the coordination process. Irrespective of those exhortations, a CXO should not need to appoint a security czar in order to achieve converged and coordinated security support for business process. Mere recognition of a department's role in a well-established and mature process should foster the convergence necessary to achieve security goals. Where simple assignment of responsibility does not seem adequate to prompt cooperation, role recognition can be formally achieved using security process documentation. As depicted in Figure 5-4, tone at the top should provide input required to document security objectives. The documentation is used to create a security roles matrix. The matrix identifies which organizations must create or participate in security process. The process definitions provide input for training requirements. As people perform the security responsibilities on which they have been trained, measurements may be taken to demonstrate whether process is being followed, as well as whether security objectives are met.

For example, say there is a central Security Program office that is directly charged with documenting policy, roles and responsibilities delegation, security training, security-specific system implementation, and incident investigation. Overlay those tasks onto the security management cycle from Figure 1-2, and shade the steps in the cycle to roughly correlate to the percentage of the activity in the step is performed in the central security group, versus others in the organization. The result will look something like Figure 5-5.

Then overlay Figure 1-2 with the names of other departments within the organization that complete the activity in the step. Once a diagram like

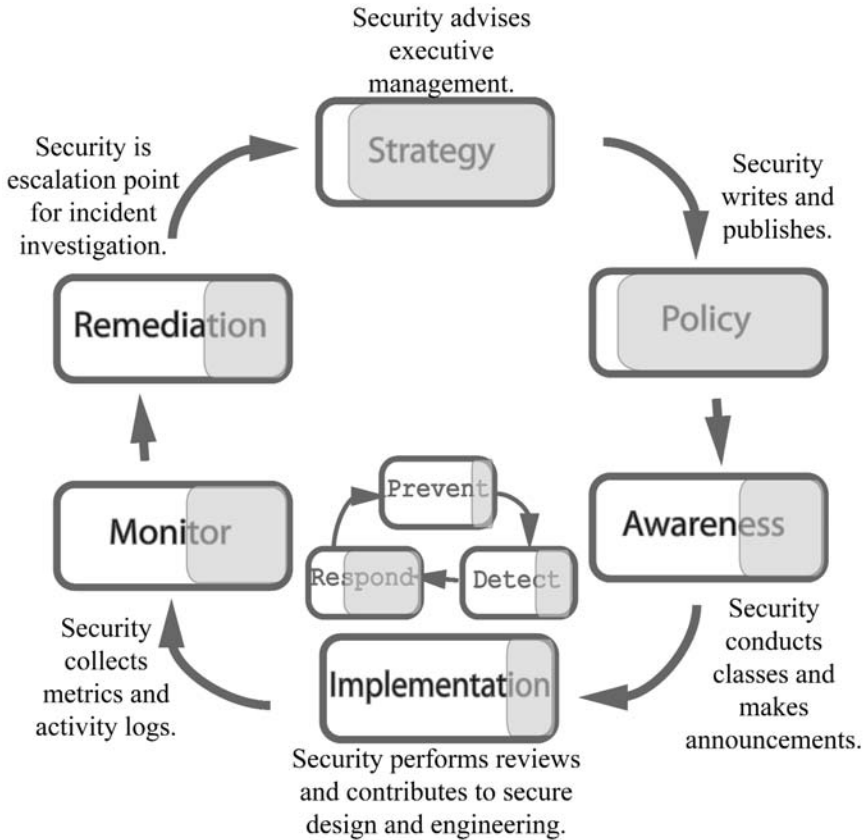


Figure 5-5: Example Security Group Roles. Adapted from Bayuk, Jennifer, *Stepping through the Security Program*, ISACA, 2007.

Figure 5-6 is published as the agreed-upon strategy by which to accomplish a Security Program, it becomes very hard for the designated departments to shirk their responsibility. Where there is still ambivalence about what the designation of responsibility means, the central security group can assist in the creation of ever more granular process and procedure until the security activity is unmistakably integrated into the day-to-day operation in the targeted department.<sup>4</sup>

This is where a little tone at the top can go a long way. Organizational effectiveness professionals who have studied the people, process, and technology dimensions by which security is usually achieved have recommended a fourth element: organizational strategy and design.<sup>5</sup> In order to be effective, organizational strategy for security must reflect the culture

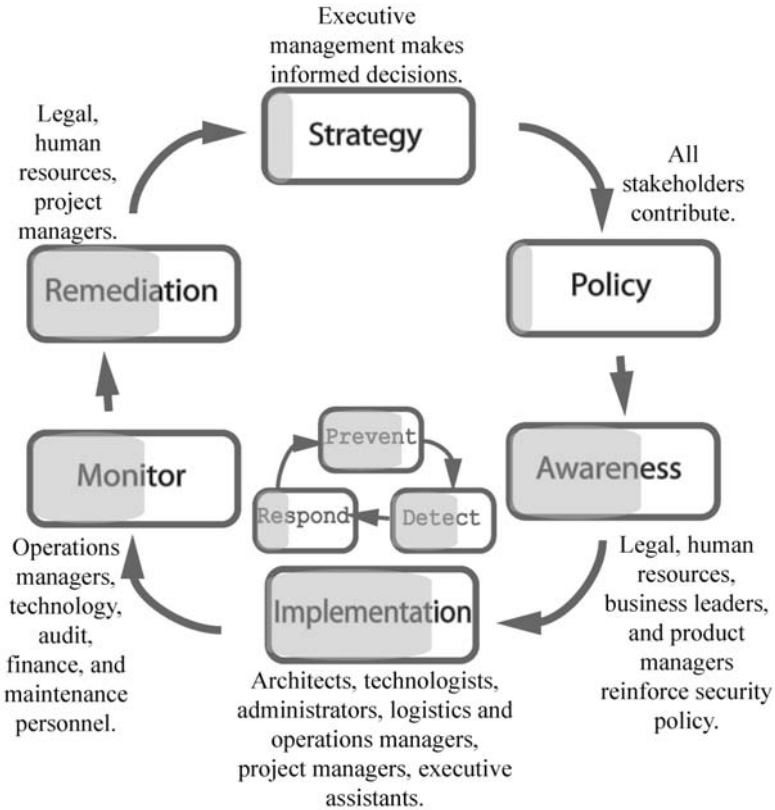


Figure 5-6: Example Matrix Security Roles. Adapted from Bayuk, Jennifer, *Stepping through the Security Program*, ISACA, 2007.

and governance processes already engrained within the organization. By making it clear that the organizational strategy and design for security has its origins in CXO mandates, a CXO can deputize every manager to play a significant role in security policy enforcement. Security Program role(s) should be included whenever and wherever there is a reference to a job function. A CXO should task the human resources department to put a line in all performance reviews whereby managers attest (or not) that the person being reviewed follows security policy. A CXO should fire people who willfully avoid compliance with security policy. Whatever tone at the top exists should be employed to make sure everyone knows that the CXO is serious about the Security Program.

*This page intentionally left blank*



## CHAPTER 6

# NAVIGATING THE REGULATORY LANDSCAPE

For a CXO to appreciate the current state of security, the most accurate perception is to see security as an attribute of the asset landscape. In the context of regulatory requirements, however, security means *management control* over the asset landscape. These perceptions are complementary. The idea is that the extent to which management controls assets is the extent to which they are secure from harm due to accidental or intentional damage or misuse. There are two aspects of management control relevant to regulatory security auditors. The first is whether or not a CXO actually has control over the organizational processes that handle assets. If a CXO does not have management control over the organization, then the organization will fail the audit. It will fail because, even if it is secure today, there is no assurance that it will be going forward. The second aspect of management control relevant to regulatory security auditors is whether the CXO uses management control in efforts to comply with regulation. If a CXO has control, and is using that control to try to do the right thing, then the organization will usually pass audit, even if it sometimes makes mistakes.<sup>1</sup>

The first aspect of management control relevant to regulatory security auditors, that a CXO is actually in charge, is achieved through security measures. Whenever a regulator examines a business process, there will be a need to show evidence that management controls that business process. Where that business process includes control points, the combination of people, process, and technology contributing to the integrity of

those control points will be in the scope of the audit. Of course, it is not always the case that regulatory audits are very thorough, but a thorough regulatory audit will test the full extent of the security controls, including all confidentiality, integrity, availability requirements.

## **REGULATORY DOMAINS**

A CXO who has set tone at the top and created an organization that understands accountability for countering threats is well poised to detect the next generation of threats to the business, and well ahead of peers in that regard. Even so, there may be something that the CXO did not perceive as a threat, perhaps because it was not a threat to the CXO's business, but to some third party protected by a regulatory umbrella. For example, the Health Insurance Portability and Accountability Act (HIPAA) is a regulation that protects the privacy of patient health records in the United States. A CXO considering the threat landscape may not have identified those records as potential targets. To catch such gaps among the regulated, regulatory auditors create their own version of the asset landscape, map security control points to it, and identify gaps that may indicate lapses in regulatory compliance.

The domain of a regulatory audit may be anything from personal financial information and health care records to nuclear power plants and building maintenance procedures. Only if a CXO has established control points within that regulatory domain can management show that they control the assets within it. When regulatory auditors come into a place of business to audit a given domain, they always have a predefined idea of what the control points should look like. As much as it can be argued that they may be looking for the wrong things, or not focusing on the right things, there is no way to dissuade the regulatory auditor from their perceived mission. From the point of view of the regulatory agency, there are not enough auditors and too many regulated entities. Moreover, they need to treat each regulated entity fairly. They must devise standard procedures for examinations and each entity will be equally subject to them.

The most important thing to know about regulators and their domains is that they are set by law. A common security profession analogy for regulators is that regulators should be treated as God; that is, the ultimate authority with respect to issues within their domain. Advice on how to deal with regulators has the ring of the first few steps in a 12-step program to rid oneself of addiction. The advice is to give up to a higher power,

don't blame others, and meet with people in similar situations and share coping strategies. Though the submissive ring does not resound well with CXOs who are risk-taking leaders, the 12-step analogy is nevertheless a good way to think about regulatory compliance. It should be beneath a CXO to argue with regulatory authority or blame external factors for not having previously considered some matter of interest to regulators. From the regulatory auditor's point of view, it would appear that the CXO is clinging to a self-destructive pattern of behavior.

The most common form of regulatory audit comes in the form of a checklist. An audit-opening meeting is the usual venue wherein a regulatory auditor reads off the checklist and asks questions to determine what the organization's control points look like, and then makes lists of control points that seem worthy of closer examination. The closer examination may consist of documentation review, interviews with personnel, physical inspection, and/or automated testing.<sup>2</sup>

## **SHARED STRATEGIES**

As auditors move from company to company, filling out their checklists and examining controls, they cannot help but see patterns in the responses. They also cannot help but form opinions on which type of controls points seem like the best evidence that their checklist items have been covered. That is why meeting with peers who are also undergoing audits is a helpful thing for an auditee to do. If an organization has dedicated security personnel or internal auditors, they should be sent to industry conferences to make sure that they are getting the best available information about what measures similar firms are taking to comply with regulatory requirements.

Not only should security and audit staff reach out to their peers via industry associations; they should collect business cards. Those cards may come in handy for the potential moment that they do not have a control point that an auditor is sure should be industry standard. Note that, although auditors see a lot of companies, they do not always see any one in great detail. They may sometimes misinterpret evidence presented in support of a control point to mean something other than it does. They may also make assumptions about how control points work together to achieve a management objective, and these assumptions are sometimes wrong. A quick call to a peer who has recently undergone the same audit can clear up a lot of confusion as to where an auditor got ideas as to what security was industry standard. SHS23 provides an example.

**SHS23:**

---

Running down his checklist for an annual review, a regulatory auditor received the same responses from the security officer that he had the previous year. Reading from a list of notes taken the previous year, the firm's security officer was on the lookout for changes. When the change came, it was puzzling. The auditor asked, "What vendor's firewalls do you have installed on your network periphery?"

As they were still in the interview process and had not gotten to the point of testing controls, the question seemed too detailed, but the security officer answered. The next question was, "And what vendor's firewalls do you have installed on your internal network?"

The security officer answered the question, and then, respectfully, expressed puzzlement. "That seems an odd question as we are not yet at the testing stage. Can you tell me what led you to add that to the checklist this year?"

The auditor responded that he has been analyzing the network at a similar company in the Midwest and that it occurred to him that if there was a flaw in the vendor firewall software on the periphery of the network, and that flaw was exploited, then all the firewalls on the internal network could be exposed from the outside. "One would have to assume," the auditor said, "that if the inside firewalls were also from the same vendor, then the entire network was at risk due to a single security flaw."

The security officer almost laughed, but kept it to a smile. "No, that assumption does not follow," he instructed, "there is no network route from the periphery firewalls to the internal firewalls, so exploiting the periphery ones would not give an intruder access to the internal ones. You would actually have to compromise another type of system to make the hop to an internal network, and those other systems all come from other vendors already." The auditor was satisfied with the explanation and moved on.

After the meeting, the security officer called his peer at the Midwest firm. The peer had also been asked the question, but had not inquired as to why it had been asked. The peer was unfortunately not as well versed on network routing, and had not thought to call in network engineers when the auditor asked him the question. He had immediately taken the auditor's suggested vulnerability as valid, and had already ordered his internal firewalls to be replaced with a different brand.

SHS23 illustrates the fact that the auditor is not always speaking to the expert in the organization on the topic being discussed. In particular, whoever is attending the initial meeting in which the checklist is reviewed is not necessarily the person with the best answer on whether the control points are in place. If that person is not completely knowledgeable in a subject matter area, the best response is to write down the control point in question and ask for a reschedule or a break, whichever the audit schedule allows. As a CXO, it is never a good idea to designate one organization as a sole “audit liaison” without empowering them to bring in all the subject matter expertise they need from the rest of the organization. The audit liaison will quickly be in over his or her head, and auditors are likely to perceive hesitation or fact-finding delays as evidence of management confusion.

On the other hand, if the auditor is dealing with a subject matter expert, that person must be careful to understand the full context of the regulatory rule under scrutiny before claiming that any given security measure meets the audit requirement. While subject matter experts can be quick to point out compensating controls, if the auditor stays the ground on a given control point, a regulated entity undergoing a regulatory audit must always take it seriously. The severity of enforcement action for violations of regulations varies with the degree to which the entity has either willfully ignored or purposely violated a rule. To challenge an auditor on why a given security control point is relevant could be perceived as a willful violation of whatever rule is supported by the security measure, and so is never the right response. There is always a polite way to ask for an explanation without it coming across as if the control point is meaningless.

The preventable part of SHS23 is that the Midwest firm spent unnecessary dollars replacing firewall hardware for no reason. The change created unnecessary work for network engineers and unnecessary complexity for the network operations. The last thing a CXO wants to do is overspend on unnecessary controls. There are always more actually useful additional controls waiting for the same dollars. The situation to be on the watch for is often referred to by affected personnel as “too much security.” This is a situation wherein there are so many barriers placed in front of an asset that even authorized people cannot get anywhere near them in a reasonable amount of time. This is antithetical to the security requirement for availability, and is thus an oxymoron.

**SHS24:**

---

A firm ordered an audit of financial systems in preparation for an initial public offering. The auditor found that there was no formal process by which users were authorized to have access to systems. The auditor recommended that the IT department produce a paper form. The recommended form had a list of the types of systems access available in the company. Managers would be expected to check off which types of access their new employees needed, and sign the form, to indicate their approval, before access was granted.

The IT department created the form to the auditor's specifications (see Figure 6-1). The form had checklists for every possible software application and hardware peripheral any user in the company had ever requested. None of the managers understood the form, but IT would not provision a user unless the form had been completed, signed, and delivered to the IT department. Managers rarely selected the right choices from the list of access types. The difference between the time at which a new employee or contractor came in to the firm, and the time at which they were set up with systems access increased exponentially with the different types of IT services they needed. The IT department merely blamed audit.

The chief operating officer then brought in a security consultant. The consultant listed typical systems access required by each department and had the CXO of each department approve the department access list. Thereafter, detailed approval was required only in special cases. Even those who had special access needs were immediately approved for the department default.

SHS23 and SHS24 illustrate that the experience auditors have in analyzing peer organizations can influence both the audit plan they use and the recommendations they make at the next organization. Other influences on an auditor's thinking are best practices documents and lessons learned at industry seminars. Where auditors are following best practice documents, it is hard to dissuade them. Unfortunately for the industry, the best practices are not justified by any actual case studies that they provide better security. Instead, best practices are often written by consultants and professional authors to describe the way security professionals would like the world to be. This allows the security professionals to use auditors as a way to achieve ideals. Consider the example of SHS25.

Firm Name \_\_\_\_\_

**Information Technology Access Request Form**

*Note: All access requests must utilize this form!*

Date Submitted: \_\_\_\_\_ ADD  Employee   
 Date Required: \_\_\_\_\_ CHANGE  Consultant   
 Expiration Date: \_\_\_\_\_ DELETE  Other

Requestor: \_\_\_\_\_ Request on behalf of: \_\_\_\_\_  
 Department: \_\_\_\_\_ Department: \_\_\_\_\_  
 Phone Number: \_\_\_\_\_ Manager: \_\_\_\_\_  
 Existing LAN ID (if any): \_\_\_\_\_

**Hardware**

- Cell Phone
  - Computer
  - Fax Machine\*
  - Headset
  - Laptop
  - Mobile Email Device\*
  - Monitor
  - Phone
  - Printer
  - Voice Mail
  - Wireless Headset
  - Wireless Network card\*
  - Other
- Please specify: \_\_\_\_\_

**Software**

- Communications Suite\*
  - Data Access Tools
  - Desktop Standard
  - External Access\*
  - File Transfer\*
  - Graphics
  - MultiMedia
  - Project Management
  - Sharing Center\*
  - Source Code Control
  - Other
- Please specify: \_\_\_\_\_ *Note - all licenses must be purchased prior to install!*

**Physical Access**

- Headquarters
  - Physical Plant
  - Data Center
  - Local Office Only
  - Other
  - Please specify: \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_ *\*Compliance approval required.*

**Email**

- Preferred handle: \_\_\_\_\_
  - Delegate Access to: \_\_\_\_\_ LAN ID: \_\_\_\_\_
    - Calendar - Please circle: read create edit delete
    - Contacts - Please circle: read create edit delete
    - Email - Please circle: read create edit delete
  - Other
- Please specify: \_\_\_\_\_ (may require additional approval)

**Files - Note - share owners will designate access level.**

- Share access - Please list: \_\_\_\_\_
- Create New: \_\_\_\_\_ List LAN IDs: \_\_\_\_\_

Authorized Signature: \_\_\_\_\_ Authorized Signature2: \_\_\_\_\_  
 Full Name: \_\_\_\_\_ Full Name: \_\_\_\_\_  
 Title: \_\_\_\_\_ Department: \_\_\_\_\_ Title: \_\_\_\_\_ Dept \_\_\_\_\_

Figure 6-1: Access Control Form

**SHS25:**

A consortium of regulatory agencies in a given industry all had overlapping regulatory jurisdiction over a similar set of companies. They agreed to consolidate their audit plans so that the same audit would be done no matter which regulatory agency performed it. The approach was meant to be more efficient for both agencies and auditees and was universally endorsed. A committee of agency auditors

drafted an audit plan and encouraged companies within the industry, the auditees, to comment. Rather than provide comments attributable to a company, the auditees delegated the comment response to existing security committees within an established industry association.

The industry association committee members included security professionals who had moved between jobs at the regulators, to the regulated companies, to the industry associations, and back, managing all the while to concentrate their careers on their security credentials as opposed to their business credentials. The resulting audit guidance mandated that there be an executive security professional appointed within each regulated entity and that the security professional should report to the company's board of directors. During the public comment period on the proposed best practice, an observer commented that this was not actually the case in the majority of the regulated companies. The committee chair on the industry association side was unfazed: "then they are not in compliance" was his only response.

The moral for a CXO in SHS25 is to watch out who represents you in industry consortiums, because if they don't understand your objectives, having representation at all will backfire. The preventable part of SHS25 is that the regulators were extremely open about the objective of the regulatory guidance and extremely willing to listen to industry expertise. The representatives from the industry could have emphasized the importance of *Security through Matrix Management*, a technique that actually was in place and working in the various regulated entities. But instead, they pushed for regulation that the head of security should report higher and higher up on the food chain within their own organizations. The result is that the level of compliance with that checklist box is low and organizations feign compliance via matrix organizational structures for reporting up (like the separatist organization in SHS21) rather than a top-down organizational structure for actual security management.

## COMPENSATING CONTROLS

Both SHS23 and SHS24 illustrate the fact that auditors' security checklists are just guidelines for the audit. It is always possible for a well-secured



organization to pass security audit using control points that are different from those the auditors expect. However, where there is recognition that the rest of the industry has adopted different control points for the same business process, an auditor cannot be expected to immediately recognize that the ones in place within an organization that took a different approach may be just as effective as those in the rest of the industry. Instead, the first recognition will be that they are nonstandard. It is good idea for a CXO to prepare the staff for an audit by telling them that it may be a challenge, and that they should assume the auditors have just come from hundreds of peer organizations that all have some control points for which their own organization has no use. The burden will be on the staff to demonstrate that the organization is in compliance with the control objectives anyway. The idea is that there should always be evidence that control points underlie compliance with each control objective, and these must be demonstrable whether or not they are assumed to comply with some industry standard.

When it does, in fact, occur that a control point in the organization is not standard, compliance entails demonstration that there is a *compensating control* in your organization that makes the expected control point less necessary. The phrase *compensating control* was invented by auditors to allow for the fact that sometimes there are situations in which it seems obvious that a standard set of control points should be in place, but they are not possible given the unique way in which some business operates, so other alternative nonstandard control points take their place, which *compensate* for the expected ones not being there. It can be as simple as whipping out a hose where a fire extinguisher was expected.

## COMPLIANCE REQUIREMENTS

The importance of understanding the objective of an audit can never be underestimated. The audit scope will be dictated by the objective. Auditors are nothing if not precise and to the point. Audits without crisply stated objectives are distained by the industry as *witch hunts*. No self-respecting auditor following standards of professional ethics would participate in a witch hunt.<sup>3</sup> Unless an audit is in fact a disguise for some covert operation, it should always be possible for a CXO to request and receive a clear audit objective in writing.

No matter what the audit objective, there should be a clear path to understanding how the auditor's approach meets the audit objective. Because of this, a good way to prepare for a regulatory audit is to have the

staff perform an internal security review using the same objective. This should make them keenly aware of what evidence may be produced to demonstrate that the required control points are in place. Methodology should be set into place so that the evidence is continuously generated and readily available. Though it takes some amount of work up front, this will minimize the time spent in staff responding to audits. It will also clearly demonstrate that management is in control.

Of course, security staff who have frequently communicated on people, process, and technology alternatives with their peers will always be better equipped to explain why they chose a given set of security measures. Wherever there is a regulatory agency, there is an industry association representing the regulated. Though these organizations may be dominated by lawyers and dedicated to lobbying efforts (and are sometimes overrun with bureaucrats, as illustrated in SHS25), they are still good sources of networking opportunities. The key is to keep the security staff focused on the business objectives for security first. They should be instructed that the primary goal of their participation is to influence regulators to ensure security regulations are consistent with CXO strategies for security. A secondary goal is to learn from others, and a CXO should be open to the possibility that these lessons may, in turn, influence CXO strategy.

Of course, the role of legal in the regulatory compliance framework should not be minimized. Though it occasionally occurs, it is not common for security professionals to have risen through the ranks of an industry-specific legal profession, so if the regulatory requirements are not a priority for the legal department, then they will likely not be incorporated into the Security Program, despite security staff participation in industry forums. Lawyers need good networking skills and opportunities as well. This is especially the case where regulators do not show up and audit, but instead periodically emphasize the importance of regulation by judicial action. The U.S. Federal Trade Commission (FTC) is one example. The sheer volume of regulated entities prevents it from considering audit as its primary enforcement methodology. But as illustrated in SHS13 and SHS14, it nevertheless has broad powers of investigation. There are countless cases wherein corporate lawyers appear not to have kept up with the latest developments via industry publications supplemented by peer networking. Where they miss obvious regulatory requirements for security and instead argue fruitlessly that their firm took appropriate actions, the company loses not just the regulatory settlement, but years in litigation costs as well.<sup>4</sup>

And, of course, everyone is subject to their local building inspector. Close contacts with local municipalities and law enforcement agencies

can be invaluable in ensuring that all security bases are covered. The actual list of security regulations that apply to a given regulated entity should be a joint project between a legal and a security professional. It should be analyzed and formulated into a crystal clear set of requirements for its Security Program.

## COMPLIANCE VERSUS SECURITY

Once the regulators and associated requirements are identified, a CXO should assume that these regulators are the “higher authority” on what practices should be in place within their own firm. Simple acceptance of this fact fosters a compliance-mindset that will facilitate all comparisons with current business practice and those that may be recommended by a regulator. It prepares the potential auditee for dealing appropriately with the mechanics of the audit and supervisory process. However, the “higher authority” perspective from the point of view of regulatory compliance should not be extended to make any conclusions about the extent to which security requirements are necessary to *complete* the organization’s actual Security Program.

Although regulators may have requirements for security, the focus of the requirements will usually be heavily on the consumer side of the product delivery cycle. An organization’s Security Program will have security requirements that do not present much risk to the regulators, but if not addressed, could present significant business risk. Security Programs deal with inherent risk to assets. If focused too heavily on regulatory requirements, they may end up using inefficient or ineffective control measures.

Consider the standard way that security professionals are taught to make risk-based decisions. As was described in Chapters 2 and 3, security professionals are taught to identify assets, asset peripheries, threats, existing controls, and vulnerabilities. Then they are instructed to list the potentially negative consequences that would probably result if the vulnerabilities were not fixed, and the threat was enacted. Lists are encouraged to be quantified. Items usually presented for consideration in these lists include (but are not limited to): investigation and repair time, lost productivity, lost opportunity, damage to health and safety, and reputational damage. They are taught that it is required that each item in the list be associated with a probability that the threat will be enacted in such a way that results in those consequences. A loss expectancy calculation is made, as illustrated in Figure 6-2. As briefly mentioned in the Introduction, there are

countless variations on this theme, and the overall approach is flawed. Nevertheless, it is widely used and there is nothing handy to replace it. So a CXO should keep in mind that this is the way security professionals are trained to think. Figure 6-2 is more detailed than the example in the Introduction. But it is a high-level view compared to most studies in the economics of security. Yet the bottom line is always the same: a security professional is challenged to come up with security measures that would reduce the vulnerabilities, and thus minimize negative consequences. The cost of those measures, combined with whatever negative consequences cannot be avoided, is compared to the first loss expectancy calculation. The basic lesson is that the cost of security measures is justified based on the probability that monetary loss will be averted. This basic methodology is actually a security industry international standard.<sup>5</sup>

For the sake of argument, say that a security professional is encouraged to believe that regulatory compliance is the primary driver of the information Security Program. The assets, threats, and risks in the calculations stay the same. But the consequences list is reduced to include only those matters of interest to regulators. Depending on the regulatory environment, these may not include proprietary trade secrets, personnel considerations, lost productivity, or a wide variety of costs to the business. They include customer satisfaction only where negative consequences include regulatory enforcement issues.

Moreover, even the regulatory requirements that are directly audited cannot be assumed to be met just because an organization passes the audit. This is a fact at least partially because there are not enough qualified security auditors in the world to do all required audits, and also because most organizations are happy to be audited by unqualified staff—so long as the unqualified auditors err on the side of allowing the auditees to pass. It is also often the case that security professionals' concentration on narrow sets of audit requirements instead of broadly applicable management controls will allow an organization to pass without having truly met regulatory requirements. A consulting firm that specializes in data breach investigations found that 19 percent of clients suffering data breaches claimed audited compliance with industry standards for protecting the data in question, but that only 5 percent of them actually were.<sup>6</sup> As one security luminary recently stated in reference to a widely applicable security audit standard, "There are 50 things you have to do but one of them is not figuring out what the right thing to do is."<sup>7</sup>

The beauty of risk management exercises is that they show a company considered risk when making decisions about security. As illustrated in

- Asset = Value of Asset
- Threat = Probability that a threat to the Asset will be enacted
- Vulnerability = Vulnerability that allows Asset to be damaged by threat enactment
- Damage = Monetary cost to firm consequent to harm to asset, includes recovery cost as well as intangible and productivity losses due to misuse and/or lapse in Asset availability
- Loss Expectancy = Expected monetary loss due to Threat enactment = Threat x Damage (probability x cost of damage)
- Fix = List of security measures intended to reduce the Vulnerability, hence also reduce the probability that threat enactment will cause Damage
- Fix Cost = Monetary cost of implementing fix
- Post-Fix-Threat = Probability that a threat to the asset will be enacted, given that the Fix has been implemented, it is presumably a lower probability than the original Threat value
- Post-Fix Loss Expectancy = Post-Fix-Threat x Damage (probability reduced by "fix" risk reduction measures x cost of damage)

**Security Risk Decision-Support Calculation:**

If ( Fix Cost + Post-Fix Loss Expectancy ) < Loss Expectancy  
 Then Implement Fix

**Example:**

- Asset = Information on Laptop
- Threat = 80%
- Vulnerability = Laptop is in possession of traveling salesperson
- Damage = ~\$100,000 in privacy litigation settlements
- Loss Expectancy = 0.80 x 100,000 = \$80,000
- Fix = Encrypt laptop disk
- Fix Cost = \$50
- Post-Fix-Threat = 5%
- Post-Fix Loss Expectancy = 0.05 x 100,000 = \$5,000
- \$50 + \$5000 < \$80,000 → **Fix Should be done!**

Figure 6-2: Example Loss Expectancy Equation

Chapter 4, the ugliness of them is when the risks are acceptable to the business, but not to its customers. Having risk calculation numbers that are focused on regulation brand the professional security exercise as: *good enough for government work*. It passes regulatory audit. But it does not secure the asset landscape. A CXO should not lose sight of the fact that the enterprise Security Program does not exist to benefit regulators. Its purpose is separate and distinct from the regulatory process. It is to secure the enterprise. Security and regulatory compliance are two separate objectives. The way security is managed and the way regulatory compliance is managed are completely different. Regulatory compliance can be managed using checklists. Security cannot.

Compliance with a rule or regulation may provide a feeling of security akin to the comfort the *Peanuts* character Linus derives from his security blanket.<sup>8</sup> Linus lives in an environment that allows him to wander through the world of *Peanuts* relatively unscathed. His wanderings have always been accompanied by his security blanket, so he associates his sense of security with the blanket. The fact that his world is so safe is actually what allows him to hold onto his security blanket. A clean audit report is like the blanket. A CXO can get an extra feeling of comfort by holding a clean audit report. However, where the Security Program covers only regulatory audit scope, there will be parts of the neighborhood that are not safe for wandering, whether or not the security blanket remains intact.

## CHAPTER 7

# INVESTIGATION AND REMEDIATION

The most important thing to know about corporate security investigation is that it is nearly impossible to do unless planned in advance. In the absence of modern-day security monitoring measures, corporate crime generally supplies very few clues as to its origin. Of course, there may be witnesses, and criminals may leave traces of activity. But unless you have Sherlock Holmes for security staff, they will probably have very few leads on actual suspects. Corporate security staff rely heavily on automated monitoring techniques, both physical and cyber. They rarely even interview potential witnesses.

The reason for the low expectation with respect to forensics by corporate security staff is simple. Corporate security does not have the same rights to investigate as does government law enforcement.<sup>1</sup> At least in the United States, private security staff are not allowed to directly challenge individuals based on suspicion. They can only detain someone upon direct observation of crime in progress. They are not allowed to handle evidence; they must instead simply preserve it for examination by law enforcement. They may collect names and addresses of witnesses who voluntarily provide contact information, but they cannot compel witnesses to provide it. The corporate security mode of operation is to set in motion as much automated evidence-collecting apparatus as possible, and hope it is enough to capture evidence of whatever harm to assets may occur.

Furthermore, despite the seamlessly integrated technology that seems quite plausible by today's standards, and is demonstrated in any number of movies involving corporate security technology, there is no off-the-shelf way to integrate evidence from the widely distributed identity databases, video cameras, alarm systems, and computer logs to pinpoint a suspect in real time. Although numerous vendors market Security Information Enterprise Management systems, which they call SIM or SIEM, there is no real definition of any actual collection of evidence that the security industry agrees should be in a SIM. Technology industry observers call this type of obscure product label "marketecture," because it is a marketing concept that alludes to systems architecture.<sup>2</sup> Like "Web 2.0" and "cloud computing," security log analysis concepts like SIEM are promoted by vendors that have partial solutions, while the actual technology that would support fully realized product vision is not readily available for purchase. Enterprises struggling to keep up with the latest innovations in investigation technology are required to develop their own solutions using combinations of commercial and custom technology products and services.

## MONITORING

Consequently, a CXO who wants to have an internal capacity for security investigation must start by funding technology projects. If a CXO is by nature optimistic and has actively nurtured a culture of trust and cooperation, then it may be a tough decision to support a security investigation staff with expensive custom monitoring systems. An optimistic and trusting CXO must first overcome the tendency, referred to in Chapter 4 as *depth-of-denial*, and admit that something bad may happen to the organization. A CXO should keep in mind that the possibility that a criminal may get away with crimes against the organization could feasibly create a *depth of outrage* that is also very hard to face.

An evenly dispersed set of centrally controlled monitoring equipment may be sufficient to deter potential perpetrators from enacting the most egregious threats, and at the same time, catch a few unanticipated mishaps as well. Criminal investigations are often aided by corporate security sources. For example, a highly publicized investigation into multiple murders of women who advertised massage services on the Internet was facilitated by evidence collected from the Internet site as well as the hotels in which the murders were committed.<sup>3</sup> The ability of these businesses to assist law enforcement in prosecuting the criminal activity that occurred



within their asset perimeters was very reassuring to their customer base. Security monitoring is also perceived as goodwill by the community at large. Monitoring that is uniform over the entire asset landscape is the easiest way to pinpoint the source of new and unanticipated vulnerabilities and exploits. As one highly regarded security professional puts it: *always expect the unexpected*.<sup>4</sup>

Nevertheless, it is understandable that a trusting CXO may hesitate to monitor assets, because, after all, monitoring assets entails monitoring the people who have access to those assets. Done without obvious context, the introduction of monitoring into a currently unmonitored environment may leave people feeling both distrusted and unfairly targeted. Nevertheless, some level of monitoring is always justified in the context of being able to detect harm to assets, so in the context of a Security Program whose other activities are consistent with the prevent-detect-respond approach, monitoring measures will quickly be taken for granted as just another asset-value-preservation strategy.

Done correctly, monitoring should do more to ease the mind of honest individuals than it should cause disgruntlement. Correctness, in this case, means that monitoring is continuous and cannot be stopped or have its integrity threatened by those whose activities are monitored. It is important that evidence of monitoring be systematically tracked via automated, or at least extremely predictable, procedures. Predictability makes it possible for those that control the monitoring process to testify as to the integrity and accuracy of the evidence it produces. Where monitoring evidence is required for legal investigations, its delivery to the legal process should be well documented, showing that each person or system that handled the evidence has not tampered with it in any way that would not be detected. The term *chain of custody* with respect to evidence refers to each point at which control over the evidence is transferred to a distinct individual. Where integrity over monitoring evidence and corresponding chain of custody is maintained, honest people will always be exonerated by monitoring. They will usually accept the trade-off with respect to privacy, as long as it can be justified by asset preservation.

A monitoring process that is operated by one set of individuals, yet observes activities of a distinct set of other individuals, is an example of a situation referred to in the security profession as a *segregation of duties*. For an easier example of the concept, consider the situation in which two keys are required to open a single lock, and each key is entrusted to a different person. The segregation of the two tasks of the single lock-opening function provides more assurance that the lock will not be mistakenly

opened than if it was a single task that could be executed by a single individual. The reason why segregating the lock-opening tasks is thought to be more secure is that there will be at least one other person monitoring the activity of whoever opens the lock. This means that unauthorized activity will require collusion. Collusion is considered by fraud professionals a moral roadblock for some people who would otherwise engage in unobserved unethical behavior.

That said, there are also many documented examples of whole teams of individuals conspiring against a perceived injustice at work.

### **SHS26:**

---

Two file clerks in a corporate litigation department recognized that some of the litigation was against employees who were “either hassled by the company or trying to get back at them for injury claims.” The clerks recognized that they routinely handled court notices that informed company lawyers of the court dates for these proceedings. They also learned that if the company lawyers did not show up for the proceeding, the case would be forfeited and the employee would automatically win. In an act of both altruism for colleagues and revenge against the corporation, one of the clerks made a habit of bundling up the notices and disposing of them while the other one watched.<sup>5</sup>

SHS26 demonstrates that monitoring should be supported not simply by segregation of duties, but also via reduction of motive among those doing the monitoring. In an ideal monitoring situation, the people doing the monitoring know little or nothing about the assets being monitored or the motivation of others to compromise the assets. They should know only that they are accountable for systematically performing the monitoring procedure, and that their own performance of the procedure is also continuously reviewed. They may not even recognize asset damage as they are monitoring, but may simply be responsible for creating monitoring records for a subject matter expert’s later review. Their lack of knowledge with respect to the assets should lessen the likelihood that they will attempt to collude with the people who are motivated to compromise the assets.

A CXO’s first encounter with security monitoring is usually just after a security horror story has occurred. A CXO who knows about or suspects

a security breach will often be curious as to what evidence may be available to identify a suspect. However, in the absence of actual breaches, a CXO can still imagine a situation in which a breach may occur. Context of an actual or imagined breach can focus a dialogue with the security team. It is a good way for a CXO to gain conceptual understanding of how (or if) the security function is organized to perform investigations.

## **INCIDENT ANALYSIS**

In a discussion of breach investigation, the best possible situation to encounter is one wherein all an investigator need do is look at monitoring logs to see exactly what happened. Of course, this type of investigation can happen only if the security staff anticipated a given type of threat and implemented corresponding detection processes. They may not have done so, which may come as a surprise to a CXO. Still, the context of a specific investigation will provide a good framework for the CXO to understand the reasons and issues involved.

A CXO should also be aware that information on current investigation capabilities versus potential capabilities is often blurred. That is, a CXO participating in discussions on the next steps of a potential investigation may be presented with alternative next steps in a somewhat equivocal manner. In order to make a decision on whether a potential investigation result is worth the level of staff effort, a CXO needs to have a very clear picture of what it is possible to learn, given the people, process, and technology in place today, versus what it may be possible to learn if the security staff went into crisis mode and took the affected departments with it.

For example, when a staff member says, “We can do that,” a CXO may hear, “We can do that now.” However, the equivocal nature of the word “can” leaves the security staff member with a buffer. They may be thinking, “We can do that if we use your authority to divert a lot of people from their day jobs to help with this investigation.” Or they may be using the second definition of the word “can,” in which case, the phrase actually means, “We know how to do that,”<sup>6</sup> but does not necessarily imply that present capability exists. Using a third definition of “We can do that,” it could mean, “We have the right to do that, even though we may not be able to handle the logistics.”

Handling this type of equivocal response is, of course, a core competency of a good CXO. Nevertheless, with respect to security investigations, the point deserves special emphasis. The amount of time and effort

it may take a security group to make the leap from “We know how to do this” to “This is done” is usually exponentially longer than it is for any other department. By the nature of the job, they are working through a matrix management structure. The process to be monitored may be something with which they are unfamiliar. The security group may need to enlist subject matter experts and technologists to assist. If increased monitoring is expected to occur without the monitoring target becoming aware that the monitoring in the environment is being changed, it becomes exponentially more difficult yet.

Table 7-1 lists six statements that a security investigator might use interchangeably.<sup>7</sup> In order for a CXO to make sense of investigative capability, these phrases must be well-defined enough so that everyone who utters one of these statements actually is accountable for saying the same thing. Specific clarification on phraseology will be appreciated by the security professional. It allows the CXO to become more of a collaborator than a dictator of outcomes, which are, by the nature of the job, uncertain enough. Consensus on nomenclature facilitates agreement that the right investigative approach is being taken with an eyes-wide-open acceptance that the goal of the investigation may not actually be achieved. It should also prevent frustration that a CXO may have with the inherently uncertain nature of the investigative process.

Even with an appropriate level of monitoring in place, a CXO will rarely have all the forensic capability required to investigate complex cyber crimes. Unfortunately, the state of the art in cyber-forensics is not anywhere near what it is in physical security. Though you can record a computer screen, you cannot run the video and see everything that happened within the computer. Basic forensic capability in cyber security provides simple file reconstruction and routine file movement through networks. Even research in the field of forensics with respect to cyber security is heavily concentrated on reconstructing data.<sup>8</sup> Cyber-forensics is not likely to address more subtle versions of the confidentiality, integrity, and availability triad, such as authenticity (where the information came from), unless highly sophisticated technical security measures such as digital signatures and transaction tracing were established over data in advance.<sup>9</sup>

The field of cyber-forensics is also not focused on reconstructing perpetrator behavior. So even with the help of the most sophisticated technical experts, it is extremely difficult to recreate an incident timeline. The level of analysis necessary is that which identifies the root cause of the incident. Incident analysis should also allow a security professional to identify controls that would prevent the incident from happening again.

**Table 7-1**  
Translation

Statement	Recommended Meaning
That is done.	All the people, process, and technology required are in place and the process has been successfully tested.
We can do that.	All the people and technology required are in place, but there is no process implemented and nothing has been tested.
We have begun this.	We have planned for the process, and are in the midst of gathering the people and technology required.
We know how to do this.	We think we have the people and technology required, but we have not come up with a process to accomplish it.
We will be able to do this.	We have a theoretical plan to accomplish it, and the plan has been funded.
We expect to do this.	We recognize this is important, but are limited by resources and have not started planning for it yet.

## INVESTIGATION VERSUS REMEDIATION

Where known incidents are not thoroughly investigated, and followed by remediation, additional incursions should be expected. SHS27 provides a good example.

### SHS27:

From 1998 to the present, NASA computer systems have suffered a variety of security incidents due to Internet hacking. Consequences of these attacks included a satellite diverted off course, supercomputers being physically unplugged from the network, and theft of data on rocket engine design, space shuttle operations, and financial planning. Some of this activity was linked to network addresses in Taiwan and China. In 2002, there was so much evidence against one malicious hacker that a federal indictment was issued. Yet there was no viable remediation activity. Rather than take a holistic approach to remediation, there is evidence that NASA officials instead retaliated against whistle-blowers.<sup>10</sup>

Where there is such obvious damage to assets, as in SHS27, remediation is required by fiduciary due diligence. Remediation is what you do to make sure a similar incident does not happen again, or if it does, that the result is less damaging. Even in cases where the incident investigation is fruitless, remediation should at least include adding additional identity tracking and monitoring to make sure that, the next time, there is more evidence to facilitate the investigation. It is no longer possible for a CXO to cling to *depth-of-denial*, because the bad thing did in fact happen. That it happened does not statistically reduce the probability that it will happen again, as in the *lightening does not strike in the same place twice* scenario. Rather, the threat becomes unavoidably visible. The fact that a security incident has occurred usually increases the certainty that it will happen again. To not act in response is to be neglectful (and thus an unfair business practice, according to the FTC, as discussed in Chapter 6, though somehow government entities such as NASA escape such verdicts).

That said, in the absence of an immediately recurring exploit, remediation does not have to be an immediate knee-jerk countermeasure. Remediation can involve sending the security strategy committee back to the asset-threat landscapes and performing a diligent reexamination of the security overlay. Additional preventive measures may be holistically applied to cover more assets than were damaged by the incident. Monitoring procedures may be changed in a variety of ways. Response procedures may be systematically rewritten throughout the organization.

From the point of view of a CXO, the difference between investigation and remediation may sometimes be blurred, as both seem to form a continuous set of activity that comes under the heading of security. This is especially true if the same people perform both processes. This situation itself presents a segregation of duties issue, as investigation work may increase the level of remediation work required, and choices as to which incidents require some level of investigation may be influenced by fear of overwork. It may also happen that an incident may be overstated in order to justify over-expenditure. Many security professionals are fond of the phrase, "Never waste a good crisis."<sup>11</sup> Remediation work should therefore always be referred back to the implementation side of the security management cycle. A Security Program may have to be enhanced to facilitate remediation work, but it is important that it have the basic capability to accomplish it with existing management process following agreed-up security objectives.

If there is not enough security leadership within the organization to accomplish remediation work, then a CXO's only choice is to bring in

consultants to do it. If the required security expertise is not on staff, the consultants are likely to come recommended from a firm's lawyers or accountants, who usually charge for referrals, so the cost will be increased. The trade-off in cost is between having a few people on staff tasked with quietly cleaning up messes, and expensive strangers coming in and having to first create a security matrix management structure in order to get the same amount of work done. A CXO that is not persuaded of the need for a Security Program in the absence of incidents will usually change opinions after comparing those costs.

## CONTROL POINT INTEGRATION

The blurring of incident investigation and remediation is even more problematic when the same set of individuals is also tasked with *preventing* security incidents. The design of remediation processes should not be solely trusted to those in charge of the processes that were exploited in the course of the incident. This itself would be a segregation of duties issue, because it is well known that those who design processes are biased in favor of their performance, and sometimes blind to their deficiencies. Moreover, a criminal who works inside the organization would be motivated to shield the process security inadequacies from investigators.

### **SHS28:**

---

A firm's Help Center received a call from an individual who was neither an employee nor a client of the firm. The caller identified himself as a security officer from another company. He stated that his company was under attack from a virus whose Internet address was registered to the Help Center firm's network. He sent logs of the activity to the Help Center via email. A Help Center technician pasted the email into a routine work order ticket, and assigned the ticket to the information security group. An information security staff member reviewed the ticket and saw that the specified network address belonged to the firm, but was not documented as one connected to the Internet. The security staff member called the network operations center and requested that they shut down the Internet address at the firm's periphery. But the network operations center claimed that the address was not on the Internet, so it could not be

part of the problem. The network operation center did, however, identify the physical location of the network port to which the address was connected. Following a documented network operations process, the information security staffer escalated the issue to the network engineering group and asked them to escort him to the specified data center location. The network engineering manager stated that their procedures prevented them from bringing anyone not in the network engineering group into the data center during the business day; all non-engineering access to the data center was to be done outside of business hours. The information security staffer protested to no avail, and escalated the incident to his management. It took a few hours before the escalation culminated in a CXO authorizing the information security staffer to go into the data center. The location that the network operations center had identified as the offending network address was empty. The security staffer called the person who reported the incident, and he verified that the virus attack had stopped about the same time the security staffer had reported the incident to network engineering. There was a camera on the data center door, but not on the location of the network address. A few network engineers had walked in and out of the data center, but none admitted to unplugging or moving equipment.

SHS28 is an example of an *insider threat*. Someone in network engineering had unauthorized equipment plugged into the Internet, and the only way it was detected was that it got a virus. That equipment was moved shortly after it was detected. However, there was not enough monitoring in place to identify the culprit. There was also not enough control over telecommunications lines to prevent the network engineers from having an unauthorized connection to the Internet in the first place. Disgruntled employees are by far the largest contributors to insider threat, but evidence shows that any person who handles assets and believes that their behavior is not monitored may become an insider threat.<sup>12</sup> At least, the likelihood is greater than for those who are obviously monitored. Fraud has its own triad: *motive, opportunity, and justification*.

Appropriate remediation activity post-SHS28 was, therefore, not left to network engineering, even though it was a network event. Departments ranging from procurement to physical security participated in planning to ensure that the network engineering group would have appropriate over-



sight going forward. The physical security remediation was particularly important because a physical security procedure had been used by network engineering management to delay the investigation. SHS28 not only demonstrates the frustration a security investigator often will have in organizations that do not have a coordinated management approach to investigation; it also provides an example of why matrix security management is absolutely necessary to provide efficiency in the security investigation process.

Requirements for coordination of investigation procedures may extend not only to various departments within the organization, but may extend to external organizations as well. A company that is dependent on service providers for safeguarding assets may also need to enlist those organizations for assistance with investigations. Unfortunately, unless investigations are routine for service providers, it may be just as hard for them as for an unprepared internal staff to come up with logs or videos that provide evidence required by an investigation process. SHS29 provides an example.

**SHS29:**

---

A firm had a workforce reduction resulting in 25 out of 40 people in a single department leaving the firm on a given day. One of the people laid off was the firm's administrator of an online service provider's Web site. A month later, the company's accountant was surprised to see charges indicating that 40 people in the department had been charged for using the online service provider's Web site. The accountant was unable to find anyone who still worked at the firm who knew anything about the online service provider's user administration process. Working through the service provider's support contacts, the accountant requested the list of active users on the site from his firm. The accountant was told that this was an unusual request, because the firm should know which of its own people used the system. It took a week to get the list. When it came, it was a list of user names and index numbers from the online service provider's system. The user names appeared to be nicknames and did not exactly match the first and last names of people who left the firm. The accountant had to make a new request to the service provider to see the first and last names that had been entered into the service provider system, and requested logs of the month's activity in the

system as well. It took two weeks to receive the additional data from the online service provider's support staff, with the consequence that the company overpaid for use of the system by two months, and three of the former employees had actually still been using the system in that time interval.

SHS29 illustrates the importance of including requirements for service provider investigation capability in service level agreements. In many cases, these investigative capabilities will also be regulatory requirements to perform due diligence on vendor handling of assets because those assets are material to the firm.<sup>13</sup> Where prevention and detection controls are also included in these due diligence exercises, investigation and remediation processes are usually easier to integrate.

If a CXO encounters a situation in which crimes against an organization are egregious, it may be tempting to attempt to retaliate. This is a frequent occurrence in organized crime communities in both physical and logical realms. What must be understood is that retaliation reduces a CXO process to the criminal level. Moreover, like any war, there will be mounting escalation as each side tries to defeat the other. This type of activity is better left to law enforcement. Advance planning with appropriate law enforcement contacts should be a core competency of any Security Program.

Where an incident response planning process is nurtured with a little CXO strategy and direction, security staff will also be establishing a general crisis command and control structure that can support any aspect of the organization. This does not have to be hierarchical, or hub-and-spoke with tentacles everywhere, but could be based on the starfish model, one in which the loss of a leg does not jeopardize the organizational structure.<sup>14</sup> A fully coordinated approach to incident management will include not just physical and logical security, but legal, public relations, and operations. Especially in cases where the incident is public-facing, it is rare that potential incident response processes will not require immediate cooperation among numerous areas of the organization. A CXO who supports a coordinated security incident response capability will in the process facilitate the development of secure communication and crisis management processes, tools that may be wielded in a wide variety of circumstances other than the typical security incident.

## CHAPTER 8

# THE RIGHT STUFF

A CXO looking for the right person to lead a Security Program should be aware that there is no precedent for a correct way to make a choice. One thing all security management positions have in common is that they are all different. Corporate security has not historically played an influential role in the business environment. There is no standard training that can be expected of leaders in this field. As one widely respected security professional observed with respect to corporate security:

Today's leaders in the security field are all converts to it from other fields for the simple reason that when we began there was no training available. This will soon change as we are replaced by people with formal training, but when that happens, the renaissance quality of security will yield to the excellence that comes from crisp specialization. This is not bad, but it is different.

Because this change will happen, it is imperative that we mine all the insights, all the ways of thinking we can from those other fields while they are still fully represented by the presence of trained practitioners from them in the security field. We simply do not have the time, and should not spend either the time or the coin, to re-invent what is already known elsewhere and can be applied here. Civil engineers know why bridges fall down, lawyers know the difference between policy and enforcement, doctors know the terrible demands

of making life-and-death decisions under uncertainty, public health practitioners know that the great triumphs over disease began with sewers not with antibiotics, preachers know that great thoughts cannot be transmitted without the vehicle of familiar tales in which to embed the higher principles, and so on. This mixing of background traits is what, in nature, would be called hybrid vigor. Hybrid vigor only lasts one generation; we must spend it with as much wisdom and perspicacity and dedication as we can muster.

When it is gone, it is gone.<sup>1</sup>

Though the observation is true, given the pace at which the hybrid vigor is melding into a security officer at the CXO level, the formation generation may last a few years longer than usual. Although the title chief security officer (CSO) has been taking hold since the mid-90s, there is not yet consensus on the amount or content of formal training that is required to assume the role.<sup>2</sup> The integration of security functions at the executive management level is following the path taken by the chief information officer (CIO) role that preceded the CSO's ascent to CXO level. Though the CIO title has been commonplace for 20 years, there is still a wide range of corporate responsibility that could feasibly be assumed by a CIO that often remains distributed within other areas of the business. Such is also the case with a CSO.

One major difference between CSO roles is that some organizations have merged physical and logical security functions into one department, and others have separate chief information security officers (CISOs) and chief physical security officers (CPSOs). There may also be departments within an organization that unilaterally appoint a security officer to handle one aspect of security for which they are primarily accountable. In most cases, the differentiation may be historical and reflect the major responsibilities of a department to which the security officer reports. For example, it is not uncommon to see a CPSO in a department in charge of facilities or building services. This also explains the advent of chief privacy officers (CPOs) residing in legal departments and security risk officers residing in financial departments. Once an organizational evolution has resulted in multiple security officers who all seem likely CSO candidates, any merging of the functions carries with it the same organizational disturbances that result from any other executive turf battle. A physical security specialist may object to "reporting to a geek," while an information security specialist may object to taking direction from someone whose expertise is "guns and guards." In most organizations, CISOs,

CPSOs, and CPOs live comfortably apart in different departments, joining forces in committees of mutual interest within the context of a matrix-managed Security Program. Only in cases where they form competing Security Programs, or start overlapping committees requiring the presence of the same set of members, should a CXO start worrying about organizational economy and efficiency.

CXO-level personnel choices are always hard, and they always depend on some melding of the skill set of the people at the top of their own organizations. If there is a great candidate to lead the security organization that does not have enough background in the industry to make decisions on information classification, that part of the job may safely be left to the CIO who has been in the industry for 20 years. If the candidate is lacking in requirements analysis, it may be a good idea to have an experienced member of the legal department be appointed as “chief privacy officer” in order to fill the gap. A CXO seeking a CSO should focus on skills and experience specific to security that may currently be missing in the organization. A CXO should look to close vulnerabilities, not to relieve other executives from their current security responsibilities. As the security function requires a matrix-managed organization anyway, a qualified CSO will be comfortable working as Security Program coordinator within a qualified team.

Qualified security professionals are like any other type of manager. They have won friends and influenced people, sought total quality management, gotten to yes, thrived on chaos, adopted seven habits, reengineered their processes, measured down their defects, managed difficult personalities, and moved their own cheese.<sup>3</sup> What they have not done is adopted a checklist approach to security, and they have not implemented programs for the sake of regulatory compliance rather than for securing assets. The checklist approach is one wherein a CSO enumerates policy requirements, makes lists of projects to implement security measures, and manages the set of compliance projects.

Another variation on the checklist approach is for a new CSO is to use tools or hire independent auditors to find vulnerabilities, and then establish projects to fix them. Professional advice columns, especially those funded by vendors selling audit software, often advise a new CSO to find as many vulnerabilities as possible and create cost-benefit-analysis calculations to justify projects to fix them. CSOs who follow this advice embark on their new jobs by telling security horror stories to the CXO in order to get funding to do projects. It is not uncommon for a CSO on a conference panel to boast that the reports provided to the organization’s

CXO are referred to internally within the security department as “the scare deck.” The scare deck is a PowerPoint presentation where each slide is a different category of vulnerabilities, and each category is followed by a price tag. Those that are not funded cease to be the responsibility of the security department to address. A CSO that uses a scare deck in order to plan security does not actually have control over how security is managed, just over the set of funded projects.

Although it is important to know about vulnerabilities, a Security Program whose major focus is to find and fix vulnerabilities is no better than a policy or regulatory checklist one. The list of vulnerabilities becomes the checklist and diverts attention from the critical business of designing and building a robust Security Program. Rather, it is the job of the CSO to work within the business to establish and manage a sound Security Program. A CSO should be a trusted confidant, capable of partnering with a CXO. The CXO should be able to assume that vulnerabilities will be appropriately addressed as part of the Security Program’s management process.

The checklist-CSO usually ends up feeling disadvantaged because the program is not working no matter how hard he tries. This phenomenon is so typical that there is an analogy for it within the security profession. It is called the *security hamster wheel of pain*.<sup>4</sup> A wheel of pain is a reference to ancient and medieval servility where slaves labor on turnstiles or prisoners are attached to torture mechanisms. The caged hamster, however, voluntarily embarks on the spinning wheel and continues to run as the wheel turns faster instead of trying to get off. A CSO who treats security management as a set of remediation projects without creating the management program around it will fail. He may work harder and faster, but will never get anywhere.

A CXO should use whatever interviewing techniques have worked over the years to weed out candidates who intend to bring a “policy checklist” or a “vulnerability audit” approach to their new security management job. If they think they already know how the job should be executed, then they probably are not qualified to do it. They may, of course, be good technicians, or qualified auditors, but they will need to learn the business before they can hit the ground running as a CSO. They should be using a “Triad and True” approach rather than a “Checklist and Covered” or a “Find and Fix” one.

Even security professionals who understand the appropriate approach may not know how to go about making it work in an organizational structure that is strange to them. Many CSOs who are new on the job have a

## The Hamster Wheel of Pain

An Alternative View of "Risk Management"

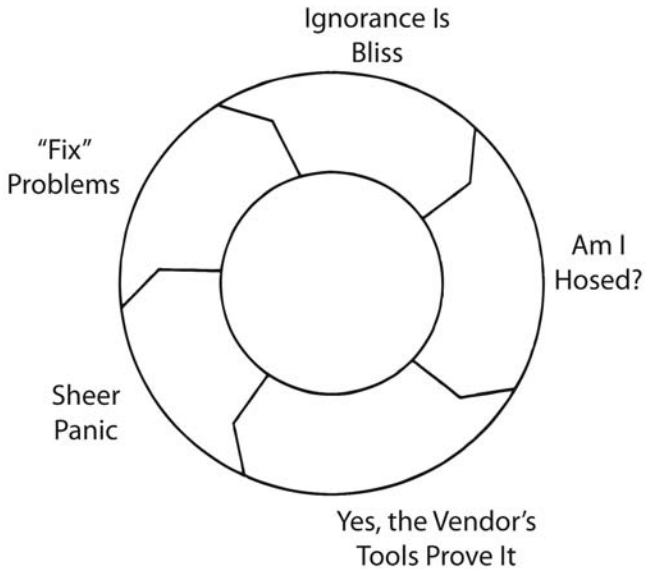


Figure 8-1: Hamster Wheel of Pain. Source: Jaquith, Andrew, *Security Metrics*, Pearson Education, 2007, page 3. ©2007 Pearson Education. Used with permission.

common story. The executive who recruited them spent a lot of time and effort finding the right cultural fit. They were honored to be chosen through such a diligent process and they are excited about the opportunity to serve under such supportive management. They have met their peers and are comfortable with their level of understanding. So they take the job. Three months in, they still have not gotten a security policy passed, or established a committee with the authority to pass one. Yet they are called into every meeting that smells of security. They are constantly being told security horror stories and helping managers fix them, but have no responsibility that allows them to create a comprehensive Security Program. Every recommendation they make adversely affects some business process, and there is no oversight to ensure that newly implemented controls actually achieve long-term objectives.

In this situation, a CXO has not hired a security manager, but instead has hired an internal consultant. The consultant is engaged solely to provide countermeasures. A CXO who brings in security talent to raise the bar with respect to asset protection must remember even seasoned security professionals are affected by tone at the top. They will provide just as much security as they think the CXO is ready to personally support. Exit interviews with failed CSOs often yield phrases like “tired of being a cop” and “it was hard walking around when 400 people can’t stand you.”

A CXO should also understand that no one can walk into an unfamiliar business, no matter how skilled they are at security, and come up with a Security Program that is meaningful to those already immersed in that business. The asset landscape is the bare minimum information a CSO will need, but it is not nearly enough. A recently retired veteran of the security profession wrote that the current state of security practice is comparable to a time when most doctors were general practitioners rather than specialists and most lawyers were community-based rather than practice-based.<sup>5</sup> Yet, he lamented, there is dire need for highly specialized surgeons. Security people should not simply be aligned with the business, they should be part of it.

### **SHS30:**

---

A recent high school graduate landed a job as an intern at a bank. She was a straight-A student with a reputation for honesty and integrity. It was a small local bank, and automation was not as sophisticated as it is today. Her job was to take a big pile of checks that had come off an automated sorting machine, separate those that were for the same account, and place them in an envelope which had a window exposing the name and address on the first check. The student found the job very boring as she continued to stuff envelopes for days on end. She quickly realized that when she missed separating the check pile by a few account numbers, no one noticed. Not only did no one notice, but her job went a lot faster. She was soon praised for how quickly she got the job done. It took the bank a few weeks before several calls from angry customers alerted her supervisor to the fact that there was a systemic issue with the student’s job performance. The supervisor confronted the student with the fact that she had not separated the customer’s checks carefully, and had thus sent some customer checks that belonged to others. The stu-



dent was honestly surprised by the rebuke. She had never had a checking account, nor had she seen an account statement. She sincerely claimed that there was no way for her to anticipate that getting a few checks in the wrong envelopes was such a big deal. Once she was alerted to the fact, she performed the task flawlessly.

The lesson in SHS30 is that, while you can teach someone what to do, and even emphasize why they are doing it, you cannot teach them how to think about it. Only in rare cases where the CSO has a depth of industry experience should a CXO assume that a CSO truly understands how to work effectively within the business. Even then, the assumption should be frequently questioned and revisited with the changing asset landscape. So unless a CXO has a very good idea of how to train someone to look out for business interests, a CXO should look for a CSO that has at least some experience in the CXO's industry. A new CSO will still be inexperienced in the CXO's environment, but the learning curve would be less steep than it would otherwise be. However, the learning curve could still be like the one described in SHS31.

### **SHS31:**

---

A new CSO hit the ground running with established policy and clear designation of roles and responsibilities. The initial landscape analysis showed vulnerabilities in the company's dozen or so Internet Web sites. An audit team was quickly assembled to identify and document what needed to be fixed. Each Web site belonged to a different business unit. Within the first few weeks, hundreds of vulnerabilities were identified. It became clear that the CSO needed a way to assign each vulnerability to the business units responsible for fixing it. The CSO found that the development community in the business units shared a trouble-tracking system wherein user-reported software bugs were tracked, and directed the cyber-security auditors to enter each vulnerability in the system. After a few months of this work, the CSO asked for a report to see what percentage of the reported vulnerabilities had been fixed by the business unit developers. The report showed that 70 percent of the vulnerabilities were "firmwide" and had therefore not been assigned to any individual development

team. Upon investigation, it was revealed that there were three different places in the trouble-tracking system where the business unit was manually entered. Where the entry was an exact match for one of the 12 business units, the vulnerability had appeared in the corresponding development team's report. Where they had been entered inconsistently, the person who developed the reports for the CSO had created a bucket category called "firmwide." Consequently, very few of the vulnerabilities had actually been assigned to the correct development team. Those that had been correctly assigned did not contain details on the exact source of the vulnerability, just a description of it and a reference to the Web site. The developers assigned to them had trouble figuring out what to do, and many had just given up. The audit team had to retrace their steps to identify each vulnerability again, and change most of the business unit data entered for the entire project.

Successful experience in security management itself is still a relatively scarce commodity, as well as the primary prerequisite for a CSO job function, and many industries have not traditionally done a great job at security. Therefore, there may not be enough security-experienced candidates from that industry. So, to avoid situations like SHS31, a CXO may have to compromise on the industry experience side.

In a situation where security management experience is favored over industry experience, a CXO can increase the probability of Security Program acceptance by appointing a team of experienced and respected advisors for the new CSO to rely upon. As with any fiduciary responsibility, the advisors should be heavily incentivized in the success of the Security Program. The advisory team should meet with the new CSO at least once a week, and follow a formal agenda to keep the CSO on track. Over time, the advisory committee may meet less frequently, but they should stay focused at least until the new CSO is able to converse in the language of the business and demonstrate Security Program alignment with CXO objectives.

Membership in the security advisory committee itself has its own set of qualifications. Though legal and operations advice are necessary, they alone are not sufficient to mentor a CSO through an unfamiliar organizational structure. At least one or two individuals on a security advisory committee must have a firm grasp on how the business works.

It helps if they are individuals whose opinion on operations in general is respected and widely sought. Whether or not security advisors have line responsibility is secondary to their ability to recognize patterns of organizational behavior, and to gain consensus on key decisions. One author on leadership put it this way: “If you were to place a camera above the work environment of a . . . group and trace the walking paths of its members throughout the day, you’d find that there are certain places—certain offices or cubicles—that are hubs of activity. These congregation points are the homes of the informal . . . leaders. Others are approaching them all day with questions about technology, politics, and life in general.”<sup>6</sup>

Of course, despite the best of advisory teams, a new CSO may make mistakes. A CSO will not start out thinking about the company the same way the CXO does. Past experience may lead the CSO to overprotect some things and under-defend others. There may be debate within the matrix organization on specific issues or projects. Yet it is important for a CXO to recognize that an initial flurry of security debates may not be about security at all, but simply dissension due to form, storm, norm, perform cycles typical to any new matrix management team.<sup>7</sup> As illustrated in Figure 8-2, when diverse individuals are compelled to form a team, they

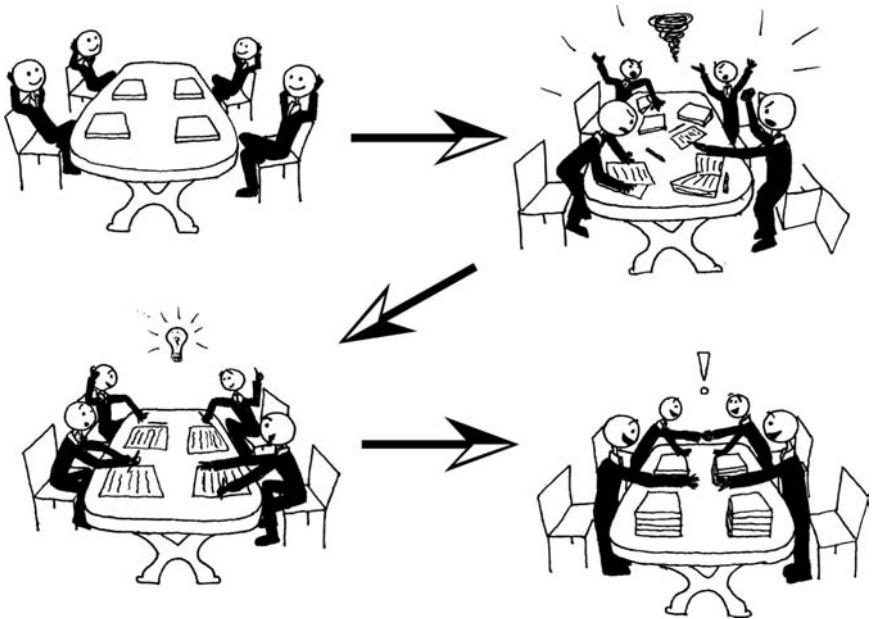


Figure 8-2: Team Dynamics

usually start out in conflict. Though the conflict appears difficult to overcome, its root cause is unfamiliar personality differences rather than any substantial disagreements. This “storm” cycle is calmed by the adoption of rules of behavior for working together, which, as professionals, they are prone to adopt. Once those rules are established and become the norm, working within them allows the team to recognize each other’s contributions, and their collective performance is enhanced. The best way to deal with debates at the early stages is to ignore them for as long as possible while periodically checking on progress toward goals. A good security management team should be able to work out most issues by themselves.

That said, there will be issues that a CSO cannot work out alone. There may be a general lack of recognition at the CXO level that security preserves value. There may be fundamental cultural barriers to preventive and detective controls. At times, a CXO may need to listen to multiple sides of a security issue and make an executive decision. These decisions will either be a sanity check on the CSO or an endorsement. Either way, a CXO can easily justify the decision to both counterparties. If it is a sanity check, a CXO need only explain to the CSO that the recommended security measure presents too much of a burden on the business process, and send the CSO back to the drawing board. A qualified security professional will accept that decision. If the decision is an endorsement of the CSO, the CXO can explain it to the rest of the staff as follows: “If we ever have to testify in court on the process we used to decide how to protect these assets, I want the CSO on the stand, not me.” A qualified security professional will be comfortable with that decision as well.

Both sanity checks and endorsements may present challenges to a qualified CSO. A sanity check may go as far as to bring in an external management consultant or auditor to assist the organization in framing a complex issue. An endorsement may result in additional responsibilities for which the CSO has no direct experience. Qualified security professionals are always comfortable with challenge. They will freely share management strategies for achieving security measures and be forthcoming with evidence on the configuration of controls. They will not hide behind mythical requirements to keep all security-related information secret, which is an all-too-common method that under-qualified CSOs use to hide their mistakes. They will welcome debate over the utility of security metrics and never rely solely on checklists to demonstrate compliance.

One way to weed out a checklist-CSO is to draft job descriptions designed to scare off the underprepared.<sup>8</sup> For example, a CSO job description might read as follows:

## Chief Security Officer

Reports to: Chief Operations Officer

Responsibilities: Direct firmwide Security Program.

### ***Details:***

Partner with executive leadership to enhance Security Program to reflect current and ongoing business objectives for security of physical and information assets, compliance with legal and regulatory obligations, and integrity of products and services.

- Distribute draft document describing enhanced program by the end of Month 3.
- Identify, evaluate, test, and assess current physical and logical security measures, including all office locations and global network connectivity within first two months. Provide documented analysis of gaps in compliance with business security objectives by the end of Month 3.

Establish controls against damage to assets, including data in transit and at rest, and all physical and logical security for all data centers and telecommunications closets.

- Establish and document technical architecture by the end of Month 2.
- Reconfigure existing equipment and staff responsibilities in support of vision by the end of Month 3.
- Plan for new equipment in project time and resource budget to be submitted by the end of Month 4.
- Execute implementation plan within budget by the end of Month 6.

Establish and maintain identity management system for all users of firm buildings and internal systems.

- Identify, procure and implement identity management system by the end of Month 3.
- Establish role and group based access methodologies by the end of Month 6 and automate access terminations based on identity management system information by the end of Month 4.

Establish and maintain facility, infrastructure, and data access control inventory. Map access control inventory to business processes. Maintain firmwide data flow that identifies technology access control points. Minimize data access by third parties and perform due diligence on third party handling of data.

- Identify and procure, or build, access control inventory data repository by the end of the first year. Establish and monitor processes for

continuous inventory data update as part of both deployment and retirement processes.

- Produce monthly and on-demand building, network, operating system, application, and data access control reports for review by stakeholders by the end of the first year.
- Support self-service online business queries with respect to staff identity and access rights by the end of the Year 1.

Establish Global Incident Response Desk in the ITIL model.<sup>9</sup> Incident Response Desk should be the first point of contact for all security issues (including customer security issues). Desk should accept requests via online forms or phone calls, and facilitate escalation for unanticipated problems.

- Identify and procure and implement source identification, trouble tracking, and log management systems commensurate with the size and scale of the firm internal staff and customers by the end of Month 6.
- Establish metrics by service request type by the end of Month 2.

Partner with business unit leaders to identify, test, and assess business recovery plans. Maintain metrics on plan strategies, including business recovery point and time objectives for each business process.

***Requirements:***

Required competencies include security process management, respect for business objectives, innovative problem-solving, organizational team-building, excellent verbal and written communication skills, sound technical skills, appreciation for economy and efficiency, and commitment to results. Candidate is expected to have at least ten years experience in security management and a degree in a technology related field. Firm industry experience preferred.

Anyone who applies for this job is either a security wizard or eager to soon become one. To distinguish those wannabes from the real thing, ask candidates what they would have to learn in order to accomplish various results. Those that think they know it all are not qualified for the job. This simple statement of fact reflects the state of the security profession just as much as it acknowledges that mysteries are inherent in the act of joining a new organization. A qualified security professional is comfortable with the fact that hybrid vigor has yet to yield the best of breed.

# CONCLUSION

Security is about management control. The extent to which a CXO controls assets is the extent to which others cannot use them in unexpected ways. A CXO who establishes a functional (as opposed to dysfunctional) Security Program can make decisions about who has access to what and for what reasons, and rest comfortably that those decisions are enforced. A CXO who has not established a Security Program can issue directives on who should have access to what, but will have no assurance that these directives are followed, and there will be a high probability that they are not.

With control requirements also comes balance. There is no such thing as 100 percent security. Executive protection measures in private industry rarely justify the cost and inconvenience that are justified in governments. It is almost always possible to continually improve security measures. In limited circumstances, there may be a business reason to be flexible about control over assets. A CXO who understands the value of a baseline (*out-run the friend*) level of security will be able to have a discussion on *how much is enough* with respect to highly critical assets.

I have been fortunate in my security career to continually draw support from CXOs for whom control over assets was obviously a worthy cause. This is how I know that every CXO has the personal ability to weave security like Kevlar into the mission of the organization, making the entire fabric stronger. As tone-at-the-top strategies vary, what each CXO decides to do will be different. The common element is pride in the ability to avoid security horror stories. It starts with a tone at the top of *Not On My Watch*.

*This page intentionally left blank*



## APPENDIX

# CASE STUDY

This case study is optional reading. It provides an example of how tone at the top serves to motivate secure behavior. In this case study, the actions of the CEO are always appropriately in line with security goals. The CEO inherits a culture where security is not valued. His staff is not accustomed to considering security as a factor in decisions. The staff falls into three categories: those who intuitively understand the value of security; those who do not grasp it by themselves, but learn from the CEO in the course of the case study; and those who resist change. As you read through the case study, identify the group membership of each staff member. At the end of the case study, each staff member is identified as a group member, followed by a list of the situations in the case study that earned the corresponding staff member group membership.

### DAY 1

The chief executive officer (CEO) called his staff together for the first time. He had been on the job for all of five minutes, but it was important for him to establish regular meetings. He was sure there would be a lot of decisions to be made in the next few months. Everyone had to be informed at the same level, and everyone needed to contribute to the decision-making process. By having the first meeting as soon as he walked in the door, he hoped to emphasize that the staff would have to plan around them.

He greeted them enthusiastically, “As you all know, I am the new CEO, Ed Exec. I am absolutely excited about the potential of this company. Although you have been through some tough times here, I am determined not to look back,” he paused with a wry smile, “unless, of course, I am required to by pending litigation.” This brought a few nervous laughs, in which he loudly participated. “So, with the past behind us and the future shining within our grasp, our clients need us more than ever. I have to hit the ground running, and we all need to band together to stay ahead of the competition.” The enthusiasm was greeted by smiles and applause. “I intend to be a high speed train on the right track, and I need each and every one of you on board, whether it be in the engine room, the dining car, or on conductor duty. Our clients need to know you are working hard to get them safely and comfortably where they want to go.” He paused for effect, then sat down. “Although I met all of you while interviewing with the Board of Directors, I have not so far gotten a real description of roles and responsibilities at this level, so let’s start out with a round-table introduction.” He turned to the person on his left, which was Leslie, the chief legal counsel (CLC).

Leslie sat up straight and cleared her throat, “Leslie Legal, as the chief legal counsel, I handle both client and vendor service agreements, manage intellectual property rights, run regulatory compliance oversight, and generally keep us out of court.” She turned right to focus on Francis, who adjusted his posture as well.

“I’m Francis Finance, the chief financial officer,” he stated matter-of-factly. “I manage the operations and technology staff who do accounting and finance.” He turned to the next person, who was Ricardo.

“Ricardo Risk, chief risk officer. I monitor information on financial results, assets, liabilities, strategic initiatives, sales trends, etcetera, etcetera. I crunch data and create reports. I brought a set of standard ones that your predecessor liked, but I can run just about anything you can think of.” He placed a thick folder on the conference table and slid it across to Ed, who stopped it with a firm slap.

“Thanks.” They both looked to Ricardo’s right, at Irene.

“Irene Info, chief information officer, though I should not really get to say ‘Chief,’ as you’ve just heard all that Francis and Ricardo have their own systems support groups, so there are other tribes out there.” Ed frowned, but said nothing. “I run the desktops, network, and client-facing applications, anything to do with telecommunications or Internet gateways.” She turned to Sunhi.

“Sunhi Sales,” Said Sunhi, “I am not a chief either, mostly because, although I run all of sales and marketing, the CEO around here has always

led the sales force personally. I do product forecasts and roadmaps, provide requirements to IT and Ops, and generally keep the clients interested.” Sunhi shifted in his seat to look at Oleg.

“Oleg Ops, chief operations officer, at your service,” Oleg waved a salute. “I get to say ‘chief’ because nobody wants my job.” They all laughed. “I do all the client support and pick up whatever needs to be done that doesn’t seem to be within anybody else’s charter. At least, I was doing that until now that you are here. So this is a good day for me.” Again, group laughter.

The last around the table, on Ed’s left, was his assistant, Arthur. He beamed at the rest of the group, “I’m Arthur, Ed’s administrative assistant. I have been with Ed for 10 years now. I have already met all your assistants and I hope to stay in constant touch with them to keep track of schedules and facilitate teamwork. If there is anyone else you think I will need close proximity to in order to stay connected with you, please let me know.” The group smiled back in silence. Arthur turned to the agenda. “The first item on today’s agenda is to plan what time we will have weekly meetings. We can choose any mutually convenient time for these weekly meetings.”

“But we must have them.” Ed chimed. He paused and glanced around the room for effect. There was no response. “At these meetings, we will have an agenda with the customer-related issues that we need to face together, as well as other decisions to be made that week, and the action items that must be accomplished that week in order to meet our goals for decisions to be made in the coming year. Where decisions are not important enough to involve this whole team, we will delegate them to committees led by you or your staff. Nevertheless, any decision made outside of this team will be discussed here if any one of you places it on our agenda. Where decisions are to have significant business impact, a cross-organizational task force will be formed. The task force leader will provide us with daily reports on progress and issues encountered.”

The group consulted their calendars and decided to meet Wednesdays at 9 a.m. Arthur read the next agenda item, “Client issues.”

Ed looked at the blank faces around the table, “OK, who has client issues?”

A few executives started typing furiously on their PDAs.<sup>1</sup> Francis cleared his throat: “Of course, on the billing side, we always have customer issues, I really did not come prepared today to present them. I see others emailing their staff to get a quick update, but I would rather not rely on that type of presentation. Suppose we start that part of the agenda next week?” The rest of the staff looked hopefully up from their PDAs.

Ed smiled. “I’ll tell you what. This week, we list the issues that we know about on the top of our heads, and next week; we will look at the full list. It is my intention to hit the most visible first anyway. Sunhi? You must know of something.”

The rest of the group looked back to their PDAs. Arthur took notes as Sunhi rattled off some recent client complaints and Ed asked questions. When they were through, Arthur read the next agenda item: “Organizational issues.”

Ed clarified: “I am assuming that the people in this room represent closure on the firm’s top management. Is there anyone who works here that does not report to one of you, either directly or through some chain?”

Francis volunteered, “There is the head of internal audit.”

“That’s OK—they are supposed to be independent.”

Oleg asked, “What about Human Resources and Building Services?”

“Where did they report previously?” Ed asked.

“Directly to the former CEO.”

“OK, now HR reports to you, Francis, and Building Services reports to you, Oleg.”

The room rumbled with reaction, but Leslie was the first to speak, “Well, now that was too fast,” she protested, “there are reasons why they need to be more closely aligned with other business areas.”

Francis was also unenthusiastic, “And really, I have no interest in getting involved in anyone else’s HR issues.”

“The very fact that we have to use the word *alignment* to talk about how they are positioned and that one of our executives would consider them a burden means to me that HR is not serving the business well where they are,” said Ed, “If they are not integrally involved in the management goals of this company, there is a problem and they have to be reorganized anyway. Bring your issues with them here, and we will help Francis and Oleg resolve them.”

Ed looked directly at each face in the room as he emphasized, “Note that if one of you is not accountable for some decisions made within the firm, then I am. I don’t want to find out later that there is some decision-making authority out there and I don’t even know who their boss is.”

As Ed’s glance landed on Oleg, the COO piped up, “What about vendors or service providers?”

Ed raised his eyebrows. “Are there any service providers at the firm directly supervised at the CEO level?”

“Why no,” Oleg admitted, “But our web hosting provider is shared among all the departments, and they take orders from anyone. I have often been surprised by what turns up on the bills.”

“OK.” Ed indicated he understood. “From now on, you run change control over those sites. Appoint someone on your staff as the ultimate authority, and create a committee among stakeholders to help whoever it is to work out the rules. And, Ricardo, I also want you to commission a task force on vendor management. I want to see a complete list of all firm vendors, risk-ranked, and each should have a responsible employee supervision contact. As I said about task forces, we should all have daily progress reports until you can produce the list.” Again, there was an audible reaction in the room, but this time no one spoke. “Anything else?” The staff seemed to be thinking hard, but for a few seconds there was only silence. “OK, now Francis and Ricardo, tell me why the CIO doesn’t centrally and efficiently manage finance and risk systems.”

Francis and Ricardo gulped. Irene rescued them. “We used to run IT centrally under the former CIO. Unfortunately, service levels were so bad that he got fired, and when I came on board there was so much to fix on the customer-facing side that I am afraid that my staff was not very well *aligned* with finance and risk. Francis and Ricardo petitioned the former CEO to separate the technology staff, and it’s been like that ever since.”

Ed turned to Oleg. “What do you think of the job Irene has done on the customer-facing side since she has been here, for,” he looked at Irene, “how many years?”

Oleg had no need to gulp, “She has been here three years and they have just been fantastic,” he gushed, “The clients love her. Service levels are always met. Simply great.”

Ed turned back to Francis and Ricardo, “Let’s let Irene have another try. I am going to send a memo to the staff on organizational changes and I only want to do it once. To me, it is a foregone conclusion that if we convened a committee to study the problem, they would recommend reemerging the groups anyway for the economic leverage of shared technology management staff. So instead, I want the three of you to create a task force to remerge the groups. Irene, you lead the task force and send us daily memos on progress and issues. Also, get the names of the IT managers that will transfer to you to Arthur as soon as you can.” Irene nodded while Francis and Ricardo looked at their hands.

“Anything else?” Head-shakes all around the table indicated none.

Memo

From: CEO

To: All staff

Re: Changes at the Helm

By now you are all aware that I have taken over as, CEO. You are no doubt wondering how this will affect your job function. I cannot at this point say anything about that, but I can say what type of staff this company needs to be successful. We need staff who are customer focused. We need to have accountability for staff decisions and actions. Where you are responsible for a business function, you are also accountable for its success.

To ensure that I personally am fully focused on the customer, I have narrowed my group direct reports. Hsu Humane, the head of human resources, will now report to Francis Finance, the Chief Financial Officer. Bill Building, the head of building services, will now report to Oleg Ops, the Chief Operations Officer.

In addition, in recognition of the outstanding service performed, our CIO of three years, Irene Info, will now centrally support all firm technology personnel and processes. Freddy It-Finance and Randy It-Risk will now report directly to Irene.

Throughout these organizational changes, all personnel will continue to be responsible to support the business in their respective domains in an uninterrupted manner. To support the behavior necessary to achieve this goal, I fully authorize every staff member to follow this guideline: If you are at a meeting and the organizer has not established a clear objective to be met during the meeting in the first fifteen minutes, leave. If in following this guideline, you experience any adverse management action, please send an email to me directly, describing the situation. I promise you I will deal with it appropriately.

I look forward to a long and healthy relationship.

Ed

Arthur stopped by to get instructions on the list of client issues that was gathered at the meeting. "I broke them down into three categories: billing, contracts, security." Ed sighed, "Oh, get me the closest thing you can find

to a product list with prices, send me the contracts for the clients complaining about them and highlight the clauses they don't like, and get me the security policy and org chart. Where does security report, anyway?"

"I will find that out when I look for the policy," Arthur said. "Also, you have a message from Leslie Legal on the ex-CEO's claims that he is not being paid the correct residuals of revenue based on the sales figures of his former clients. When the board asked him to leave, he negotiated a contract that gives him 1.5 percent of everything that we make from anyone who used to be his client. He claims we are sending him 0.8 percent."

Ed frowned, but said nothing. He turned to his computer. "Did you notice that when you got a computer account here that it didn't make you choose your own password?" he asked Arthur.

"Not only that, but my name is spelled differently on my physical security badge than it is on the computer. I would guess that Francis's systems use some payroll-generated record and Irene's group creates their own. We probably have an identity-management problem. But it just means you made the right decision when you told them to merge. Irene should work it out." Ed nodded.

## WEEK 2

Ed came in the next Wednesday at 6 a.m. He had not had a chance to fully analyze the previous day's task force reports and wanted to make sure he was up to speed before the staff meeting. He was surprised to find the lobby empty. Where there was usually a security guard standing near the elevator, there was instead only a janitor mopping the floors. He asked the janitor where the security guard was.

"He just hit the head, be back in a minute," was the reply.

Ed frowned but said nothing. Once off the elevator, he found the reception desk empty as well. His office, however, was locked. He wandered about and found some staff in a cube. He introduced himself, and they complimented him on his memo, which made him smile. "How do I get in my office at this hour?" he asked.

"Oh, the receptionist has the office keys in her desk drawer. When she gets here at 7:30, she goes around and opens them, but you can grab them anytime you need them from her desk. She doesn't mind."

Ed frowned, but said nothing but, "Thanks." He remembered that one of the client issue categories was "security." Arthur had been able to find nothing that looked like a security policy, but he did produce the name of

a client that complained about security. Ed looked up the client's salesperson and found it was Sanjay Salestaff, and asked him to drop by with more details.

"Typical client security audit," said Sanjay when he came in at 8:30. "These guys spend more money on their security team auditing us than they do on our product, and for them, it is just a formality. They give us a spreadsheet with 800 questions about tech and ops in it. We fill in a column with yes and no answers. Then they tell their regulators they reviewed us. To me, it seems like a ridiculous waste of everyone's time. I guess whoever in operations filled out the spreadsheet said yes when they should have said no, and now I have to resolve this myself." Again, Ed frowned, but said nothing.

He made his way to the second weekly staff meeting. He looks around the table. "What's wrong with this picture?" he asked. The staff looked at each other, down at the well-formatted agenda, at Arthur, glanced through last week's meeting minutes, and then looked back at the CEO. "Where is Leslie?" he asked.

The staff gave a collective sigh of relief. "Oh, she's just down the hall finishing up a meeting with outside counsel. She said she would be along in a few minutes." Without a word, Ed took off down the hall. In two minutes, he was back with Leslie, who looked a little shaken. They both sat down.

Arthur announced the first item on the agenda, "Client security issues."

Again, there was silence. Ed broke it with a question, "Oleg, I hear that when clients have security audits, someone on your staff provides them with the information they need to conduct them?"

"Oh yeah," Oleg said, "I know what this is. Sanjay's client was not happy with our answers to how we recovered from the fire in the Los Angeles office a few months ago. See, the recovery plan called for the staff to regroup on an empty floor or a building outside of town reserved for exactly that purpose. Instead, they had gone into a company-owned building two blocks away. The regional manager sent unnecessary office staff home early and gave the displaced salespeople their desks. Still, there was an audit finding that disaster recovery plans were not adequately executed."

"Sounds like they recovered a lot quicker than if they had gone offsite. This is not a failed audit. This is an innovative business recovery improvement effort by a quick-thinking sales manager. Who runs the business recovery process? We should be able to discuss the security audit with the client and set them straight?"



Irene answered, "It is run by a steering committee. The chair is my head of infrastructure." Ed frowned but said nothing. Irene continued, "Steering committees force people to consider all aspects of a given process, but I understand that they also may promote complacency due to lack of individual accountability. Business recovery does not have much of a champion around here. They do what they can."

Ed frowned again and said nothing. Arthur looked back to the agenda, "Agenda item number 2, client billing issues."

Everyone turned to Francis who shrugged his shoulders and looked up at the ceiling. "Why is everyone looking at me? He complained? I don't make up the numbers, I just send out the bills."

Ed believed him, because Arthur had been completely unable to come up with a product and associated price list. The contracts were all based on usage, and the charges seemed to vary. Ed's eye swept across the room, "Who makes up the numbers?"

After a period of silence, Ricardo volunteered, "Well, as the person who has been here the longest, I can testify that the current bills are individually negotiated charges based on estimated usage based on previous usage, and each month, actual usage from the month previous is reconciled with the previous month's bill. Any difference in amount is supposed to be adjusted. The programs were written years ago and run on Francis's system with a data feed from Irene's client applications. Leslie's group enters the numbers for each client when the contract is signed. See, we want to get paid in advance and charge by usage at the same time. But sometimes the numbers don't seem to work. We always just assume that there is some problem in the data feed and make the adjustment in favor of the client."

Irene piped up, "I send a usage file by client ID to Francis' group every month, but until now, I didn't know there may be problems with it. Now that they report to me, I will find out what in the process is broken."

Ed exchanged looks with Arthur, as each remembered the identity management issue they had discussed the previous week. Then he also remembered the ex-CEO lawsuit conversation that had preceded it. He turned to Irene: "OK, Irene, report back to us what you find next week before we pursue this further." He then turned to Francis. "But I am curious about something. Is the ex-CEO paid on estimates or actuals?"

"Actuals," Francis replied. "He has no access to the actual client bills, only to the reconciled number."

Arthur was quick at math and had studied the numbers, "But he is claiming a percentage based on the estimates!" he blurted.

“I don’t know how he could have gotten them unless the clients gave him copies of their bills.”

“Does he still have systems access at all?”

“Absolutely not.” Francis replied.

“Well, not so fast . . .” Irene was obviously reluctant to speak, but nevertheless had information to share. “Salespeople can see client accounts on the Internet. The client gets their passwords from their salespeople, so if the CEO kept a history, he could have that data.”

“We don’t let clients choose their own passwords?” Ed and Arthur asked the question in unison; both were honestly surprised.

Irene again spoke reluctantly, “They can, but we don’t make them. This is a business requirement from sales. They say the clients would be inconvenienced.”

Ed shook his head, “It sounds to me as if we need some security hygiene around here. From now on, we treat passwords like toothbrushes. No one shares them with anyone else, and we change them every six months at minimum.<sup>2</sup> Security hygiene also means that we all understand our roles in keeping undesirables from polluting our client relationships, our operations, our financial statements, and our reputation. Wherever you or your staff hold the keys to firm assets, you have to have something in place to know that they are not being stolen or lost. This applies to everything from client reports to office furniture. Does everyone understand what I mean by their role in this?”

After a pause, Leslie began politely, “Ed, of course you know that I do my best to advise according to best practices in information protection, but honestly, I don’t know what you think I can do about it if the business chooses to ignore my advice.”

Francis broke in before Leslie could finish her words. His voice dripped with sarcasm. “He means you should be downloading best practices documents, doing a global replace on the words *Company X*, and issuing them as our security policy.”

“No, I do not.” Ed spoke quietly and quickly, enunciating every word. “As I said last week, Leslie, you come in here with your issues, and we discuss them as a group. You don’t just drop them. You raise them. Best practices are one thing, but negligence is another. If we are guilty of negligence and you aren’t screaming your head off about it, you are simply not performing the job of information protection counsel.” Leslie swallowed and nodded.

Ed continued. “Once issues are raised, we work together to address them. Leslie, prepare a memo for the clients. Tell them their passwords will expire over the next few weeks.”

“Will do.”

“Irene, make sure the systems can do this and your service desk staff is well-trained on the process. Let me know when you are ready and I will send out the memo.”

“Roger.”

“OK, it is clear to me we need a task force to establish a Security Program. Ricardo, Irene, Leslie, and Oleg, you are on it, and, Francis, send your head of human resources as well.”

Francis shook his head. He seemed exasperated by Ed’s involvement in his domain. “Ed, if I am going to be participating in the Security Program, the last person I would have representing me is the head of human resources.”

Ed was patient. “Francis, I did not put you on the task force, but everyone will end up participating in the Security Program. Right now, I am looking for the person who will play the role of head of human resources. If whoever you have in the job cannot do that, I would suggest you replace them. But the rest of the staff has got to have transparency in where the keeper of the job descriptions lives. It should be human resources.”

Francis was still livid: “But you said you only call task forces for significant business impact issues.”

Ed frowned and said nothing to Francis. Instead he turned to Ricardo: “You lead this one, and send us daily progress.” Ricardo nodded. The meeting was adjourned.

The usually quiet Arthur could not contain his maternal instincts. He hurried down the hall after Francis. “Francis, I know Ed did not respond to you, but I know he means security *is* a significant business impact issue.” Francis glared at him.

## TASK FORCE MEETING

At 8:00 the next morning, Ricardo, Irene, Oleg, and Hsu Humane sat in the boardroom glaring at each other. All had full and conflicting calendars for the day, yet the task force had a progress memo to publish at the close of business. Hsu spoke first. “Ricardo, this is your area, why didn’t you just take responsibility and save all our schedules for the day?”

Ricardo shook his head, “Are you kidding? How am I supposed to run security when I can’t even get your boss’s staff to monitor expense reports? And I know what an expense report is supposed to look like. Besides, Oleg already has physical security under building services, how

hard could running one information security department be? Oleg, why didn't you volunteer?"

Genuinely surprised, Oleg thought for a minute. "Do I really run physical security?" He shook his head, "No, the guards are outsourced, I have nothing to do with that. Actually, I think you signed that contract, Leslie. Why not just get another one for the information side and be done with it?"

"Do you think signing a contract means supervision? If your people are not supervising those guards, then who is?" Realizing this was a rhetorical question, Leslie sighed and sat down.

Irene tried to build consensus. "Ricardo, you have a daily progress report to make. We can't just sit around blaming each other." She broadened her gaze to the rest of the group. "We need to get reconciled to the fact that we have to do something about it."

Leslie hung his head in agreement. "The truth is, we never really considered security a significant management issue. Ricardo, I agree with Oleg. This is your area. What are our risks?"

Ricardo gave some ground. "OK, you are right, I need to identify risks. But I think there is a segregation of duties issue in me running a security program. So say for now, we all just brainstorm on security risks."

Irene was the first to agree, "Works for me, I already did." She reached into a binder she had brought with her and handed a document to Ricardo, who was relieved.

"Great, can everybody else get me one of these by, like noon? I can categorize them in some comprehensible way, and at least then we have a status report by the end of the day. Then everyone can think overnight about what to do about them." With minor discussion, all agreed on Ricardo's suggestion. The first task force progress report was a simple statement that the committee had started gathering requirements for a Security Program, and included Table A-1 as an addendum.

The members of the task force were not the only people who thought overnight about what to do about the risks. Ed was initially shocked by the first security task force risk summary. He called Ricardo. "By the end of today's task team meeting, I want two more columns on that table you sent. Person responsible to follow up, and some description of what they plan to do. All those individual items now need to be tracked. Did you decide where security will report yet?" Ricardo replied in the negative. "Then get yourself a consultant to bridge the gap and start doing a sanity check on the task force's plans. Also, have them start working on the governance issues right away."

**Table A-1**  
Security Task Force Risk List

Risk Area	Security Risk	Risk Category				
		Data Leakage	Integrity or Availability	Regulatory Control	Management	Reputation
Client Application	Salespeople have client passwords.	X	X	X	X	X
	Privileged Database IDs and passwords accessible from user environment.		X	X	X	
	Finance users use Excel to manipulate financial reports post-system-generation.		X	X	X	
	Software development lifecycle not defined in risk and finance; current process allows undetected unauthorized deployment.		X	X	X	
	Some applications lack QA test environments; test processes do not require end-user involvement.		X	X	X	
	Developers have access to production application databases.	X	X		X	

*continued*

**Table A-1 (continued)**

Risk Area	Security Risk	Risk Category				
		Data Leakage	Integrity or Availability	Regulatory Control	Management	Reputation
Infrastructure	Regional admin responsibilities are not defined.				X	
	File-share access process allows mistakes to go unnoticed.	X	X		X	
	Most users have administrative access to their workstations.				X	
	Users have access to removable media devices.	X				X
	Business recovery plans do not include recovery point and time objectives.		X		X	
Governance	No asset inventory.				X	
	No security policy.			X	X	
	No security awareness activity.			X	X	X
	No investigation capability.				X	
	Few application activity logs and no log management strategy.			X	X	X

Physical	Physical security system logs not archived.					X	
	Office keys are easily accessible.	X				X	
	No ownership for physical security of data center.	X	X			X	X
	Badge system database maintenance overdue.		X				
	Video system playback not successfully tested.					X	
Vendor	Web vendor change authorization process not defined (in pilot).		X			X	
	Non-employee access not tied to Third Party relationship.	X		X		X	X
Information Protection	No authoritative source or naming convention for identity of authorized individuals.	X		X		X	X
	No established way to verify identity for users (internal or external) for password reset.	X	X	X		X	X
	User physical and logical access per job function not auditable.	X		X		X	

---

**WEEK 3**

Ed once again came in early on Wednesday. There was a guard and his office was locked. On the receptionist's desk was a note instructing any employee who was looking for his or her key to speak with an administrative assistant two doors down. The woman knew Ed by sight but still had him sign an access log before she opened his door. "This is not to identify you or cause you trouble," she explained, "just to have some evidence that my opening your door was justified. I hope you don't mind. Of course, if I did not recognize you, I would have had to look up your picture in the system, so I guess I am identifying you." She giggled nervously.

"No problem at all." Ed smiled. He was glad to see that Oleg was taking his security task force action items seriously. He carefully reviewed the task team reports.

"The first item on the agenda is contingency plans during the search for a new CFO."

Everyone looked at Ed, who said, "I know client issues should always come first, but I received Francis's resignation this morning, and you notice he is not in the room, so I may as well start out by letting you know why I am not hunting him down. Ricardo, you will obviously have to help me fill in on the supervisory side in accounting. But we have candidates coming in this week, and I hope it will be only a few months in transition."

Ricardo nodded while the others dove for their PDAs.

Ed ignored the distraction. "The next agenda item is client issues. I will start off by congratulating Irene on resolving the billing data integrity issues." Ed led a round of applause.

"Now let's talk about our marketing strategy fiasco. Sunhi, why do you think it happened?"

"Although I take full responsibility for marketing, I was blown away by what the competition already had by way of tech and ops. I was presenting our new service product as innovative and everybody else already had it. They just called it something else, like cloud services, or something. Honestly, I am not enough of a geek to have recognized the difference. I just knew clients were asking for it."

"If we aren't understanding the requirements at the tech and ops level, then we need to identify someone who can understand this, and that person needs to get into some forum that can recognize what's going on out there and teach us. Who here goes to conferences with competitors or belongs to an industry association?"



When no one responded, Ed frowned but said nothing. Reading the signal, Oleg spoke up, “I used to belong to the Invaluable Industry Association, and it was very valuable. I will renew my membership now and keep an eye out for potential. I’m sure it would not hurt for me to join their security discussion forum as well.”

“Great.” Ed was relieved. “Next issue?”

Arthur read from the list, “Client security issues.”

Ricardo started passing out a one-page graphical illustration of security task force risks, goals, and progress. “I had our new consultant put together a concise representation of where we are with the Security Program. I guess you can now say the program is in place but it has a lot of unmet goals. Irene, Oleg, and Hsu have some new security responsibilities, and we are progressing on their goals. But there are still some issues that don’t even have accountable owners. We are interviewing this week for someone to manage this. But the task force cannot agree on where it will report.”

Ed took a minute to peruse the graphical analysis before he responded. His first remark was, “We should have the consultant overlap by a few months to see how this chart improves after the new person starts.” It was greeted with a chorus of assent.

“On the reporting, can you shed any color on the task force’s progress?”

Leslie answered for Ricardo. “Everyone else thought it should be me, and I thought it can’t be because I will be setting the vast majority of the requirements and seeing that they are done.”

Ricardo defended the rest of the group. “We thought we could safely leave the watchdog duties to internal audit.”

Ed gave no indication of agreement or disagreement. “I guess CFO is out for now,” he said, turning to Ricardo. “What are the issues with having it be in Risk?”

Ricardo was prepared for the question, “We could do it. No doubt. But remember, we basically decide how everything else in the firm works. For example, we just finished up the vendor risk management metrics too, and we need to launch that program. If the security person was here, I think our own operations might possibly get less scrutiny than they should.”

Ed again did not indicate agreement, but instead continued around the table, “Irene?”

“Like Ricardo, I would be happy to handle it. But I get so flooded with priorities that I am afraid I would not give it the time it would need at the beginning. This person is going to need a lot of mentoring.”

Ed again did not indicate complete agreement, but said, “I buy the mentoring argument, but that applies to everyone.” They all turned next to Sunhi, but Ed shook his head, and they all laughed at the suggestion. Oleg was next.

“Yes, it could work in Ops,” he said. “I already have put supervision of the guard service under Building Services. But I considered that a temporary solution. Also, I would be hard pressed to support the information security side without taking staff from Irene, and you had already indicated that IT should be central.”

Ed again did not indicate agreement, but turned to the next person at the table, who was Arthur. He smiled broadly. “I’ve got it. We won’t decide. The person will report to me for now. Arthur will be the mentor. The initial assignment will be to complete the task force objectives that will build out the Security Program and give it a real home.” Arthur was obviously delighted with the suggestion, and everyone else was relieved.

Memo

From: CEO

To: All staff

Re: Security Organization

By now you have all noticed a few changes in the way we value the assets in our environment. You have discovered that the firm has requirements to identify individuals who have access to our offices and information, and to ensure that our assets are used only in accordance with business objectives. We have accomplished these changes with almost no business interruption. For that, I thoroughly congratulate our security task team: Hsu Humane, Irene Info, Leslie Legal, Oleg Ops, and its dedicated chairperson, Ricardo Risk.

This work will continue under the newest member of my staff, Sally Security. She is tasked with developing and implementing appropriate measures to protect, monitor, and investigate the confidentiality, integrity, and availability of all organizational assets. Note that Sally’s appointment does not relieve security responsibility from those who already have it. Rather, it enhances our already fully accountable management team. Please join me in welcoming Sally to the organization.

## CASE STUDY GROUP MEMBERSHIP

The actions of the CEO are always security-appropriate. His tone is consistent. The communication methods are recognized easily by Arthur, and soon the new staff catches up as well.

The staff falls into three categories: (1) Those who also recognize the value of security. (2) Those who do not understand security initially, but are trained by the CEO. (3) Those who do not get it. Without reading further, use the worksheet in Figure A-1 to identify which staff fall into what categories.

Case Study Worksheet	
<i>Match the numbers to the characters in the Case Study who most closely match the numbered description.</i>	
(1) Those who also recognize the value of security.	
(2) Those who do not understand security initially, but are trained by the CEO.	
(3) Those who do not recognize the value of security	
<input type="checkbox"/>	Arthur Assistant
<input type="checkbox"/>	Ed Exec
<input type="checkbox"/>	Francis Finance
<input type="checkbox"/>	Irene Info
<input type="checkbox"/>	Leslie Legal
<input type="checkbox"/>	Oleg Ops
<input type="checkbox"/>	Ricardo Risk
<input type="checkbox"/>	Sunhi Sales

Figure A-1: Case Study Worksheet

## CASE STUDY ANSWERS

### Staff group 1:

Arthur: There were many clues that Arthur was well-versed in security. His observation with respect to the spelling of his name in two unrelated systems made him suspect that there was not an integrated approach to

identity management issues. He was surprised that client passwords were not private. In general, he treats his security assignments with the same determination as his other tasks.

Oleg: Oleg takes over responsibility for building security and quickly accomplishes goals. He also identifies the lack of supervision for web hosting vendor as an organizational issue, and agrees to take responsibility for it without argument. In the third staff meeting, he had come to understand the significance of Ed's frowning and saying nothing. Because of this, he volunteered to attend industry association meetings and gather security requirements.

Ricardo: Easily understood how to run the vendor risk management program, the security task force, and how to produce appropriate metrics for each. He placed emphasis on the importance of metrics to the feedback loop in the security lifecycle.

Sunhi: Sunhi identified client security issues in the first staff meeting, which indicates that he treated them with as much importance as other issues brought to the CEO's attention on the first day of the job.

#### **Staff group 2:**

Irene: Though Irene was not well-versed in security, she intuitively understood that integrity of client billing data was part of her job function to enforce. However, she did not take responsibility for poor password security, but initially blamed the salespeople. However, after Ed's security responsibility instruction, she followed Ed's instructions by being proactive with respect to responsibility for systems security issues. This is evident from the list she brought to the first task force meeting.

Leslie: Leslie initially had trouble reading Ed. Clues were her tardiness to the first meeting and her difficulty in following the asset landscape discussion. But she caught on to her role in maintaining security when Ed laid it out for her. She then immediately recognized her role in communicating with clients with respect to security issues.

#### **Staff group 3:**

Francis: There were many clues that Francis was not well-versed in security and also resistant to change. At the first staff meeting, he questioned the CEO's request to discuss a topic without warning. At the second staff meeting, he suggested that it was possible for legal to fulfill their security responsibilities by publishing a best practice document. Francis also questioned the use of a task force as inappropriate to use for security, given that the CEO had stated that task forces were for significant issues. He then objected to including HR on the security task force. The fact that he is absent from the third staff meeting indicates that the CEO judged that Francis's resistance was an impediment to team success.

# NOTES

## INTRODUCTION

1. Bamber, Bill, and Andrew Spencer, *Bear-Trap*, Brick Tower Press, 2008, p. 26.
2. Axelrod, Warren, “The Dynamics of Privacy Risk,” *Information Systems Control Journal* (www.isaca.org), Volume 3, 2004.
3. Gordon, Lawrence, and Martin Loeb, *Managing Cyber-Security Resources*, McGraw-Hill, 2006.
4. Taleb, Nassim, *The Black Swan*, Random House, 2007. In this book, Taleb observes, among other things, that prior to the first sighting of a black swan, it has been agreed by experts that all swans are white.
5. As quoted by David Segal, “In Letter, Buffett Accepts Blame and Faults Others,” *New York Times*, March 1, 2009, p. 16.
6. Kiely, Laree, and Terry Benzel, *Systemic Security Management*, Libertas Press, 2006.
7. Kim, Love, Spafford, and Allen, “IT Operational Pressures on Information Security,” in *Enterprise Information Security and Privacy*, Axelrod, Bayuk, and Schutzer, eds., Artech House, 2009.
8. Masli, Richardson, Watson, and Zmud, “CEO, CFO & CIO Engagement in Information Technology Management: The Disciplinary Effects of Sarbanes-Oxley Information Technology Material Weaknesses,” University of Arkansas, April 2009.
9. In this case, one such solution would be to require computer accounts not to accept passwords that are names or words, and require them to have numbers

and special characters in them, as well as to require all user accounts to change their passwords on next login. Of course, in this case, there is probably more wrong with the security settings than just the password parameters, so a full security parameter audit should also be conducted. There are a wide variety of tools in every price range that can be applied to produce accurate management reporting on the level of control achieved by these types of security measures.

10. This phrase was made popular by a report commissioned by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control—Integrated Framework*, 1992 (see [www.coso.org](http://www.coso.org)).

## CHAPTER 1

1. Schneier, Bruce, *Beyond Fear*, Springer-Verlag, 2003, p. 38.
2. Cooper, Michael, “Shooting at City Hall,” *New York Times*, July 24, 2003.
3. Schweitzer, James, *Computers, Business, and Security*, Butterworth, 1987, p. 7.
4. For example, ISO 27001/27002, Information Security Management Standards, 2006, which are based on British Government Standard BS7799; also see the U.S. National Institute of Standards and Technology (NIST) Special Publications, a series for security professionals at <http://csrc.nist.gov/publications/PubsSPs.html>.
5. See Bayuk, *Stepping through the InfoSec Program*, ISACA, 2007, p. 65.
6. Pande, Peter, R. Neuman, and R. Cavanagh, *The Six Sigma Way*, McGraw-Hill, 2000, p. 37.
7. Drucker, Peter, *The Essential Drucker*, HarperCollins, 2001, pp. 112–126.

## CHAPTER 2

1. Pereira, J., J. Levitz, and J. Singer-Vine, “U.S. Indicts 11 in Global Credit-Card Scheme,” *Wall Street Journal*, August 6, 2008.
2. Skinner, Neil, “Thieves Cause Web Chaos,” *Watford Observer*, July 10, 2008.
3. Amoroso, Ed, *Cyber Security*, Silicon Press, 2007, p. 112
4. Cappelli, D., A. Moore, R. Trzeciak, and T. Shimeall, “Common Sense Guide to Prevention and Detection of Insider Threats, 3rd Edition—Version 3.1,” Software Engineering Institute, Carnegie Mellon University, January 2009.
5. The word *hacker* is used in the sense of the news story in SHS4. Although the original definition of the term referred to any person who was good at making computers bend to their will, mass media have adopted it to refer to those who hack into computers in order to get unauthorized access to information. With acknowledgment that those who used to be proud of being

labeled a hacker could once have claimed that hackers can be on the side of good, I yield to common vernacular.

6. Watters, John, "Threat Update," Information Systems Security Association CISO Executive Forum, Washington, DC, May 9, 2008.
7. For examples, see Acohido, Brian, and Jon Swartz, *Zero Day Threat*, Sterling, 2008.
8. Acohido, Brian, and Jon Swartz, *Zero Day Threat*, Sterling, 2008, pp. 68–69.
9. Gorman, Siobhan, and Evan Ramstad, "Cyber Blitz Hits U.S.," *The Wall Street Journal*, July 9, 2009, p. A1.
10. Smedinghoff, Thomas, "Legal and Regulatory Obligations," in *Enterprise Information Security and Privacy*, eds. Axelrod, Bayuk, and Schutzer, Artech House, 2009.

## CHAPTER 3

1. Deloitte Touch Tohmatsu Global Technology Markets & Telecommunications Industry Group *The Rise of Malvertising*, 2009 Predictions, p. 22.
2. Parker, Donn, *Fighting Computer Crime*, Wiley, 1998. pp. 238–239.
3. Shostack, Adam, and Andrew Stewart, *The New School of Information Security*, Addison-Wesley, pp. 35–40.
4. Influential examples are Peltier, Thomas, *Information Security Risk Analysis*, Auerbach, 2001; and Hardy, Gary, *Information Risks: Whose Business Are They?*, Information Systems Audit and Control Association, 2005.
5. Alex Hutton from Risk Management Insight, [http://www.riskmanagementinsight.com/toSecurityMetricsnewsletter\(www.securitymetrics.org\)1/27/2009](http://www.riskmanagementinsight.com/toSecurityMetricsnewsletter(www.securitymetrics.org)1/27/2009).
6. Bayuk, Jennifer, "Security Review Alternatives," *Computer Security Journal*, Volume 21, Number 4, Fall 2005.
7. Craig Mundie, as quoted by Acohido, Byron, and Jon Swartz, in *Zero Day Threat*, Sterling Publishing Co., 2008, p. 230.
8. For a summary of the early floppy issues, see Editors of Time Life Books, *Computer Security*, Time Life Books, 1990, pp. 67–69.
9. Worthen, Ben, "Card Data Breached, Firm Says," *Wall Street Journal*, January 20, 2009.
10. Halvorsen, Jaatun, Jensen, Nergard, and Vegge, "Fools Download Where Angels Fear to Tread," *IEEE Security and Privacy*, Volume 7, Number 2, 2009, p. 89.
11. *Information Technology, Security Techniques, Information Security Risk Management*, International Standards Organization, ISO/IEC 27005:2008(E).
12. Parker, Donn, "Making the Case for Replacing Risk-Based Security," in *Enterprise Information Security and Privacy*, eds. Axelrod, Bayuk, and Schutzer, Artech House, 2009, p. 96.

## CHAPTER 4

1. See [www.astm.org](http://www.astm.org).
2. US-China Economic and Security Review Commission, *2008 Report to Congress*, [http://www.uscc.gov/annual\\_report/2008/annual\\_report\\_full\\_08.pdf](http://www.uscc.gov/annual_report/2008/annual_report_full_08.pdf), p. 167.
3. Gostick, Adrian, and Dana Telford, *The Integrity Advantage*, Gibbs Smith, 2004.
4. Winterford, Brett, *EBay targets Romanian fraudsters*, *USA Today*, 6/27/2007. Also see [http://pages.ebay.com/securitycenter/law\\_enforcement.html](http://pages.ebay.com/securitycenter/law_enforcement.html).
5. DeAvila, Joseph, "Beware of Facebook 'Friends' Who May Trash Your Laptop", *Wall Street Journal*, January 29, 2009.
6. LaVallee, Andrew, "Marines Ban Facebook and MySpace, Pentagon Considers It," *Wall Street Journal*, August 5, 2009.
7. Wolf, Christopher, *Proskauer on Privacy*, Practising Law Institute, 2008, p. 4-24.
8. Wolf, Christopher, *Proskauer on Privacy*, Practising Law Institute, 2008, p. 4-27.
9. Smedinghoff, Thomas, "Legal and Regulatory Obligations," in *Enterprise Information Security and Privacy*, eds. Axelrod, Bayuk, and Schutzer, Artech House, 2009, Chapter 8 and Appendix A.
10. This was the Electronic Funds Transfer Act of 1978, and Regulation E.
11. See for example, J. David Dean and Andrew F. Giffin, "Enterprise Risk Management, What's Your Risk Appetite?," *Emphasis*, Volume 1, 2009, pp. 14-17 (see [www.towersperrin.com/emphasis](http://www.towersperrin.com/emphasis)).
12. See, for example, [www.stopbadware.org](http://www.stopbadware.org) and [www.spamcop.net](http://www.spamcop.net).
13. Schneier, Bruce, *Secrets and Lies*, p. 369
14. Howard, Michael, *Writing Secure Code*, 2nd ed. (Microsoft Press, 2002), p. 19.
15. Bayuk, Jennifer, "Vendor Due Diligence," *ISACA Journal* (Information Systems Audit and Control Association, [www.isaca.org](http://www.isaca.org)), Volume 3, 2009. ©2009 ISACA. All rights reserved. Used with permission.
16. This is commonly implemented via a network address check in addition to the normal login and password check.
17. Gorman, Siobhan, "Electricity Grid in US Penetrated by Spies," *Wall Street Journal*, April 8, 2009.
18. Davidson, Paul, "Cyberspies Have Hacked into Power Grid, Officials Say," *USA Today*, April 9, 2009.
19. Lai, Eric, "Identity Thieves Hit Customers at TD Ameritrade, E-Trade," *Computerworld*, 10/24/06.
20. Black, Lewis, *Me of Little Faith*, Riverhead Books, 2008, p. 66.
21. This phrase was coined by Richard Power.
22. Fahmy, Dalia, "Making Financial Data More Secure," *Institutional Investor*, January 13, 2006.



## CHAPTER 5

1. The latest developments in security metrics can be found at [www.security-metrics.org](http://www.security-metrics.org).
2. There are just 86,000 members of the Information Systems Audit and Control Association, the largest global professional association of information security professionals and auditors.
3. This term was coined by an alliance of security associations, who jointly support studies, such as Booz-Allen-Hamilton, *Convergence of Enterprise Security Organizations*, The Alliance for Enterprise Security Management ([www.aesrm.org](http://www.aesrm.org)), November 2005.
4. For examples of such security process and procedure, see Bayuk, *Stepping through the InfoSec Program*, ISACA, 2007.
5. Kiely, Laree, and Terry Benzel, *Systemic Security Management*, IEEE Security and Privacy, November/December 2006, pp. 74–77.

## CHAPTER 6

1. Of course, this lenient behavior on the part of regulatory auditors may change given the financial crisis, but as it is the first level of inspection that is most germane to security, the second is not as relevant to the current discussion.
2. For a complete guide to the information security audit process, see Bayuk, Jennifer, *Stepping through the IS Audit, Second Edition*, ISACA, 2004.
3. See, for example, the Institute for Internal Auditors Code of Ethics at [www.theiia.org](http://www.theiia.org).
4. See countless examples in Wolf, Christopher, *Proskauer on Privacy*, Practising Law Institute, 2008.
5. International Standards Organization, *Information Technology—Security, Techniques—Information Security Risk, Management*, ISO/IEC 27005:2008(E), 2008, [www.iso.org](http://www.iso.org).
6. Baker, W., A. Hutton. C. D. Hylender, C. Novak, C. Porter, B. Sartin, P. Tippet, and J. A. Valentine, *2009 Data Breach Investigation Report*, Verizon, 2009, pp. 41–42 (also posted at [http://www.verizonbusiness.com/resources/security/reports/2009\\_databreach\\_rp.pdf](http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf)).
7. Cohen, Fred, in conversation at a *Metrixon* program committee meeting, San Francisco, April, 2009. Cohen, who is also credited with the first use of the word “virus” to describe malicious computer programs that replicate themselves, has written several authoritative books on information security.
8. Schultz, Charles, *Security Is a Thumb and a Blanket*, Cider Mill Press, 2006.

## CHAPTER 7

1. Wyllie, Joseph, “Guard Service in the Twenty-first Century,” in *Effective Physical Security*, Fennelly, Lawrence, ed., Elsevier Butterworth-Heinemann, 2004.
2. C. J. Rhoads, *The Entrepreneur’s Guide to Managing Information Technology*, Praeger, 2007, p. 90.
3. Goodnough, Abby, “Man Held in Boston Hotel Killing,” *The New York Times*, April 20, 2009.
4. Fennelly, Lawrence, *Effective Physical Security*, Elsevier Butterworth-Heinemann, 2004, p. 10.
5. Sprouse, Martin, ed, *Sabotage in the American Workplace*, Pressure Drop Press, 1992, p. 62.
6. Dictionary usage cites *Webster’s New Twentieth Century Unabridged Second Edition*, Simon and Schuster.
7. Of course, this table has applicability far more broad than investigation process and, once established, could be reused in a variety of contexts.
8. See March/April 2009 *IEEE Security and Privacy* and *IEEE Signal Processing*. Both issues are devoted to forensics.
9. See Paul, George, *Foundations of Digital Evidence*, American Bar Association, 2008.
10. Summarized from Epstein, Keith, and Ben Elgin, “The Taking of NASA’s Secrets,” *BusinessWeek*, December 1, 2008, pp. 73–79.
11. The origin of the phrase is described in Rosenthal, Jack, “On Language—A Terrible Thing to Waste,” *The New York Times Magazine*, August 2, 2009, p. 12.
12. Cappelli, D., A. Moore, R. Trzeciak, and T. Shimeall, *Common Sense Guide to Prevention and Detection of Insider Threats*, 3rd Edition—Version 3.1, Carnegie Mellon University, January 2009.
13. Bayuk, Jennifer, “Vendor Due Diligence,” *ISACA Journal* (Information Systems Audit and Control Association, [www.isaca.org](http://www.isaca.org)), Volume 3, 2009.
14. The *starfish* model of leadership was described in: Ori Brafman and Rod Beckstrom, *The Spider and the Starfish*, Penguin Group, 2008.

## CHAPTER 8

1. Geer, Dan, in presentations since circa 2002. Used with permission.
2. There are a multitude of security skill-level certifications, but none covers both physical and logical security at the management level, and only one covers logical security at the management level. That is the Certified Information Security Manager certification offered by the Information Systems Audit and Control Association ([www.isaca.org](http://www.isaca.org)). In addition, while many graduate and business schools have electives in security, or technical security degrees, there is no consensus on curriculum.

3. These phrases mimic the following management texts: Carnegie, Dale, *How to Win Friends and Influence People*, Simon and Schuster, 1936; Walton, Mary, *The Deming Management Method*, Dodd, Mead, 1986; Fisher and Ury, *Getting to Yes*, Houghton Mifflin, 1981; Peters, Tom, *Thriving on Chaos*, Alfred A. Knopf, 1987; Covey, Stephen, *Seven Habits of Highly Effective People*, Simon and Schuster, 1990; Hammer and Champy, *Reengineering the Corporation*, HarperBusiness, 1993; Pande et al., *What Is Six Sigma?*, McGraw-Hill, 2002; and Glen, Paul, et al., *Leading Geeks*, Jossey-Bass, 2002.
4. Jaquith, Andrew, *Security Metrics*, Pearson Education, 2007, p. 3.
5. Rossi, John, "Integrity versus Accuracy," *Information Security Journal*, Volume 17, 2008, pp. 203–205.
6. Glen, Paul, et al., *Leading Geeks*, Jossey-Bass, 2002, p. 53.
7. The cycle is widely recognized, and was initially published in Tuckman, B. W., "Development Sequence in Small Group," *Psychological Bulletin*, Volume 63, 1965, pp. 384–399.
8. This approach has been endorsed by recruitment and retention consultants Smart, Geoff, and Randy Street, in *Who*, Ballentine Books, 2008.
9. Standard published by the Information Technology Infrastructure Library ([www.itil.org](http://www.itil.org)).

## APPENDIX

1. PDA = personal digital assistant, such as a Blackberry or an iPhone.
2. Paraphrased from a quote attributed to Cliff Stoll, security expert and author of *A Cuckoo's Egg*.

*This page intentionally left blank*

# INDEX

- access control form, 99
- accountability, 16, 48
- advisory team, 126
- always expect the unexpected, 109
- asset landscape, 13–19, 40, 47–48, 51, 54–56, 58, 67, 75, 93, 124
- attacker’s advantage and defender’s dilemma, 68
- audit, 16–17, 48, 51–52, 54–56, 93, 97–98, 101
- audit, review, assess, 50–57
- authenticity, 44
- availability, definition, 44
  
- bear analogy, 23–24, 27–29
- Bear Stearns, 2, 5, 9
- best practice, 5, 34, 47–48, 51, 98
- black swan, 5
- bridge analogy, 26–27, 72
  
- chain of custody, 109
- checklist, 47, 70, 95, 106, 121–122
- checklist and covered, 122
- Chief Information Officer, CIO, 16, 120
- Chief Information Security Officer, CISO, 120
- Chief Physical Security Officer, CPSO, 120
- Chief Privacy Officer, CPO, 120
- Chief Security Officer, CSO, 120–130
- Comedy Central*, 75
- compensating control, 97, 100–101
- compliance, 94–95, 101–106
- confidentiality, definition, 44
- confidentiality, integrity, availability, 44–46, 48–49
- configuration, 16
- control activity, 48, 54
- control objective, 48–54, 101
- control points, 40, 44–46, 48, 52, 54–56, 93–95, 97, 101–102
- convergence, 86, 89
- coordinated approach, 84–86
- countermeasure, 52, 56, 58–59
- CXO, definition, 1
- cyber-forensics, 112
  
- data breach investigations, 104
- depth of denial, 75, 108, 114

- denial of service attack, 31
- due diligence, 70, 114
- efficiency, 48–49
- elephant in the room, 5
- escalation, 20, 42, 118
- evidence, 48–60, 93, 95, 101–102
- exit interviews, 124
- experience, 124–127
- false sense of security, 48, 106
- fear, uncertainty, and doubt (FUD), 1, 3–4, 29, 33
- Federal Trade Commission (FTC), 65, 102
- find and fix, 122
- fire and forget, 13
- form, norm, storm, perform, 127
- fraud, 110, 116
- FUD. *See* Fear, Uncertainty, and Doubt
- general controls, 51
- good enough for government work, 16–17, 106
- Hamster Wheel of Pain, 122–123
- how much is enough, 47, 131
- hybrid vigor, 120, 130
- impact analysis, 35–36
- incidents, 42, 63, 74, 87, 89, 111–118
- industry standards, 53, 74, 95, 104
- insider threat, 27–28, 110, 115–116
- integrity, definition, 44
- investigation, 107, 111–118
- investigation nomenclature, 112–113
- job description, 128
- keeping up with the Joneses, 5
- keeping your friends out, 12, 17, 40, 75
- law enforcement, 27–28, 63, 107–108, 118
- leadership, 1, 9–10, 80, 119, 127
- locks, 19, 23, 35, 56, 109–110
- logical versus physical security, 45
- logs, 108
- loss expectancy, 103–105
- malvertising, 43
- malware, 64, 67
- management control, 93
- marketecture, 108
- matrix organization, 77
- metrics, 48, 58, 79
- monitor, measure, manage, 58–60
- monitoring, 107–111
- motive, opportunity, justification, 116
- never waste a good crisis, 114
- opening meeting, 95
- organizational structure, 77–91
- organized crime, 29–32
- patch, 27
- people, process, technology, 45–50
- perimeter, periphery, 24–26, 35, 68, 73
- plan, do, check, act, 21
- Prevent, Detect, Respond, 40–44
- prevention, detection, correction, 40
- privacy, 45, 65, 94, 109, 120–121
- product insecurity, 64–70
- recovery objectives, 53–55
- regulatory expectations, 93–100, 104–106
- remediation, 114–117
- retaliation, 118
- risk acceptance, 66
- risk appetite, 66
- risk calculation, 3, 20, 47, 52, 59, 64, 66, 103–105
- risk tolerance, 52, 54, 66
- roles and responsibilities, 86–91

- scare deck, 122
- scope, 52, 55
- security blanket, 106
- Security Horror Story (SHS), 1, 6, 63
- Security Information (Enterprise) Management, SIM, SIEM, 108
- Security Management Cycle, 19–21, 40–42, 44, 49, 51, 60
- security measures, 46
- security policy, 19–21, 47
- security procedure, 10
- security product vendors, 3–5
- Security Program, 6–7, 18–22, 35–36, 45–54, 59–60, 77–78, 84–86, 114, 119–123, 126, 131
- security review, 55–56, 58
- security theatre, 4, 12, 70
- security through obscurity, 70
- segregation of duties, 109–110, 114–115
- separatist approach, 82–83, 85, 100
- Sherlock Holmes, 107
- SHS. *See* Security Horror Story
- specialization, 124
- starfish model, 118
- supply chain, 61–62
- team, 127
- terrorism, 56
- threat landscape, 27–29, 33–37, 56, 68, 94
- tone at the top, 7–11, 15–17, 19–20, 36–37, 52, 90, 124, 131
- tone at the top, artificial, 16–17
- too much security, 97
- toothbrush analogy, 142
- trust, 35–36, 45, 63, 74, 79, 108–109, 115, 122
- Tylenol® case, 62
- unfair business practice, 65, 114
- unintended consequences, 14
- unwarranted assumptions, 51
- utility, 44
- vendor due diligence, 70
- vulnerability, 35, 37, 56, 73, 122
- weather, 61
- witch hunt, 101
- without which nothing (*sine qua non*), 18
- you don't have to be a target to get shot, 29

*This page intentionally left blank*



## About the Author

Jennifer L. Bayuk is an information security management and information technology due diligence consultant, experienced in virtually every aspect of the field of information security. She specializes in security roadmaps, and is engaged in a wide variety of industries with projects ranging from technical architecture requirements to security governance. She has been a Wall Street chief information security officer, a manager of information systems internal audit, a Price Waterhouse security principal consultant and auditor, and a security software engineer at AT&T Bell Laboratories. While in financial services, Bayuk chaired the Securities Industry and Financial Markets Association Information Security Subcommittee and the Financial Services Sector Coordinating Council Technology R&D Committee. Working with the Department of Treasury's Office of Critical Infrastructure Protection, she coordinated committee activities to support the Department of Homeland Security's National Infrastructure Protection Plan. Bayuk frequently publishes on IT governance, information security, and technology audit topics. She has authored two textbooks for by the Information Systems Audit and Control Association: *Stepping through the IS Audit* and *Stepping through the InfoSec Program*. Jennifer has also co-edited a collection of works on *Enterprise Information Security and Privacy* for Artech House. She has lectured for organizations that include the Computer Security Institute, the Institute for Information Infrastructure Protection, the Information Systems Audit and Control Association, the National Institute of Standards and Technology, and the SysAdmin, Audit, Network, Security Institute. She is a Certified Information Security Manager, a Certified Information Systems Security Professional, a Certified Information Security Auditor, and Certified in the Governance of Enterprise IT (CISM, CISSP, CISA, and CGEIT). Bayuk is an industry professor at Stevens Institute of Technology and has masters degrees in computer science and philosophy. She can be reached at [www.bayuk.com](http://www.bayuk.com).