Introduction to Information Security

CHAPTER 1

WHO CAN CONCEIVE OF AN organization that doesn't involve information and systems? Information created and used in organizations reflects all the intellectual property, competitive intelligence, business transaction records, and other strategic, tactical, and operating data for businesses and people. Regardless of industry, managers in organizations today need some understanding of how to protect these information resources, as well as their personnel. This is even more so the case if managers work in some form of "knowledge work," a term coined by Peter Drucker referring to work done primarily with information or work that develops and uses knowledge. Given the importance of information systems security in modern life, there is no escaping that we need a solid foundation in technical knowledge and a strong set of critical thinking and analytical skills to succeed in today's global knowledge work marketplace.

Chapter 1 Topics

This chapter:

- Gives an overview of technology and security behavior issues.
- Presents an overview of organizational governance.
- Discusses cyber crime, security, and costs.
- Provides a presentation of management responsibilities.
- Covers insider and outsider threats.
- Introduces assessment, planning, and evaluations and provides an overview of security attacks.

Chapter 1 Goals

When you finish this chapter, you should:

- Understand the relationships among organizational practices, technologies, and employees.
- Be familiar with the costs of cyber crime and security implementations.
- Know some of the reasons for attacks.
- Become acquainted with various security technologies.

1.1 Technological and Behavioral Security Issues

Many of the security solutions proposed in the literature have tended to ignore the fact that the problem of securing organizational systems has its grounding in human behavior. The fact remains that information security defenses have not kept pace with abusers' attempts to undermine them. Without the right skills, security decision-makers will continue with wasteful spending on ineffective or poorly implemented security technologies, protocols, procedures, and techniques. But there is a related insidious condition: Unused or poorly implemented security technologies and techniques are not sufficiently helping managers improve their security-related decisions, better solve security-related problems, make more effective plans, or take improved courses of action—leading to unbounded costs associated with lost strategic opportunities, tactical missteps, lost revenues from security breaches, and the myriad other problems that result from this waste.

Managers and security consultants are on the front lines of the problem because they assume special responsibilities for ensuring that their workforce takes precautions against violations to the security of people, organizational systems, and information resources. This has become even more crucial post-*9/11* (as it has come to be known) because of growing legislation and regulation of industry. For example, terms such as "downstream liability," where companies have been held liable for unwittingly having their computer resources used for illegal purposes, have been joined by the concept of "upstream liability," where consultants might be held liable for giving advice that leads to corporate liabilities.

1.1.1 Organizational Governance

The main security management issue relative to the concept of governance is in the management of ***risk***. Risk may be defined as the potential for harm or damage to be caused to people or assets from a proposed threat. We will discuss risk management in more detail later and further refine the definition, but for now keep this definition in mind so that you can frame it in your mind relative to governance. ***Governance*** is the use of best practices—those that are commonly accepted as "good common sense" in

a particular domain of knowledge and expected relative expertise, and additionally using standards and requirements for a given industry such as regulations for the purpose of reducing risks.

Depending on the industry and the role a manager holds in the organization, it is important to realize that international work laws and regulations vary widely and that the laws that affect work are changing rapidly. In the United States, the federal Department of Labor specifies many of the public policies and regulations that affect work. This body oversees regulatory agencies such as the Occupational Safety and Health Administration, Bureau of Labor Statistics, and Worker's Compensation.

State agencies such as state departments of labor may also define work regulations, and there are regulations that affect work in a specific industry such as the National Archives and Records Administration (NARA), which has created regulations under the Federal Records Act (FRA) to prevent shredding or deleting certain kinds of email. These regulations may have implications not only for email considered to be federal records but also a range of message types in the wake of antitrust litigation and the Public Company Accounting Reform and Investor Protection Act of 2002.

Also, depending on their roles in the organization, some managers may need to know how to perform risk analyses and conduct threat and vulnerability assessments for measuring levels of security risk and producing plans for risk mitigation. These actions may include the creation of disaster preparedness, business continuity, and disaster recovery plans. (Note that we will cover these topics in more detail in subsequent chapters.) Managers may even be involved in conducting criminal forensic analyses and might be called upon to assist in the prosecution of criminal activity.

Even non-technical managers need a fundamental understanding of principles and practices used in managing information and people securely. They need to understand, at least at a cursory level, security management policies and applications, and how governance models and risk management best practices factor into implementing and managing an effective information and systems security infrastructure so that proper decisions can be made—and in gaining approvals for budgets and spending, and implementing proper and measured security controls.

1.1.2 Security, Cyber Crime, and Costs

Cyber crime statistics are difficult to come by partly because of the scope of the problem and the underreporting of incidents. Some of the best guesses, however, indicate that losses grew in the United States from roughly $378 million in the late 1990s [1, 2] to approaching $1 billion by 2009 [3]. In the late 1990s, approximately 50% of companies reported having at least one security-related incident during the year [1], but by 2008, nearly two-thirds of companies reported at least one incident in that year [4]. By 2009, nearly three-quarters of companies surveyed had had security incidents in the previous year [3].

Also, lawsuits against employers and individual actors (managers, coworkers, subordinates) are dramatically on the rise [5], along with increases in suits against outside cyber attackers and blog posters [6, 7]. Concurrent with the increase in the number of incidents and lawsuits, the costs of implementing security measures has grown steadily, reaching

more than 8 percent of an average company's budget by 2006 [8], and continues climbing beyond that figure [9]. In 2003, private industry spending on information security in the United States was more than $1 billion and was more than $6.5 billion for the U.S. government. According to the Information Security Oversight Office [10] of the U.S. National Archives and Records Administration:

> The [2003] cost estimate on information security for the US government indicated a 14 percent increase over the cost estimate reported for FY 2002. For the second year in a row, industry reported an increase in its cost estimate. The total cost estimate for Government and industry for 2003 is $7.5 billion, $1 billion more than the total cost estimate for Government and industry in 2002. In particular, physical security cost estimates went up by 47 percent. All other categories noted increases: Personnel Security (1%); Professional Education, Training and Awareness (18%); Security Management, Oversight and Planning (16%); Unique Items (8%); Information Security/Classification Management (19%); and Information Technology (17%). [10]

Rapid technological changes occurring in the Internet along with new web-based technologies and social media are enabling communications in ways that are outpacing their regulation, giving rise to new issues related to "free speech" versus rights to "due process." Consequently, many companies are using what might be called ***strategic lawsuits against public participation*** (SLAPP) toward people and corporations that post negative comments about another in a public forum such as a blog or a website. The most common type of SLAPP is for defamation, but one of many alternatives has been to use tort interference against such bloggers and website posters. Although companies that file such claims hope to intimidate critics by burdening them with legal fees even if the filing party knows that the case might be dismissed at the end of a long legal battle, companies who have invested much in brand reputation are often willing to engage in this "strategic losing battle" because they know the *real* financial loser could be the critic.

Many states, especially California, have enacted some form of anti-SLAPP law to try to help neutralize frivolous lawsuits. Regardless, anyone who posts negative comments—even if it is only stated as an opinion (which is one defense against a defamation claim) should take caution. Managers should make their personnel aware that a response to their negative postings might not be in the form of a rebuttal in a blog, but rather in the form of a summons to appear in court. If the employee has made these negative posts from a company-owned system, the company as a whole may be involved in the suit—thus online governance and proper online behavior should be included in the company's policies.

On the other side of the coin relative to using a SLAPP, some "freedom of speech" proponents have criticized the tactic, but aside from the idealism of that position, the reality is that managers are responsible for protecting corporate assets that include intangible factors such as brand and corporate reputation, which affects the financial interests of the business. Thus managers have to weigh the *pros* and *cons* of striving to protect their corporate image and brand integrity through the legal system. However, it is incumbent upon management to strive to make a reasoned choice and resolve problems amicably if possible. This is one of the key pillars of risk management.

1.1.3 Management Duties, Responsibilities, and Threats

As we alluded to earlier, managers are in a vice-grip between containing costs and containing risk exposures. The tensions created by these opposing goals may force managers into certain compromises. Before making the tradeoff decisions, managers at all levels need to be both educated and informed. *Keep in mind that most management successes can be attributed to how well managers contribute to keeping the corporation profitable*. Managers carry duties and responsibilities to take prudent actions to protect their workforce and corporate assets. These responsibilities and duties encompass (among other actions) formulating and overseeing the organization policies and company practices and processes.

There are many (and the number is still growing) standards and criteria by which organizations are judged internationally [11]; we are seeing an increase in mandated regulations throughout the United States, the United Kingdom, the European Union, and all across the globe to govern organizational practices. However, even these necessary mechanisms are not sufficient to prevent security incidents. By way of analogy, as it has been said, passing a driving test and obtaining a driver's license may not be sufficient to protect one from having an automobile accident [12].

Much of the concentration in the security literature has been on dealing with outsider threats; however, a large proportion of security incidents involve insiders. We define insider attacks as *intentional computer misuse by users who are authorized to access systems and networks*. Insiders are typically employees or contractors of a corporation, although vendors, service personnel, consultants, and others may also broadly be defined as insiders [13].

Surveys indicate that current and former employees cause most of the computer attacks, that roughly 80% of those attacks were caused by internal employees, and that 89% of those attacks were done by *disgruntled employees* [14]. Detecting insider attacks can be an extremely difficult problem, but predicting them might be even more challenging. Because past behavior is a good predictor of future behavior [15], managers may examine past conduct by using pre-employment screening and background checks to help predict behaviors. However, there is always the possibility that an offender has not yet been caught, and so employers may monitor and evaluate employees continually on the job. Note that managers need to balance three "legs of the chair"—that is, (1) try to filter out anyone who is not a good fit or is a risk, (2) monitor critical behaviors for workers on the job to help prevent or intervene in deviant behavior, and (3) undertake appropriate actions in response.

1.2 Assessing and Planning

A critical managerial function is to assess the exposure of assets and strive to provide a value for those assets to the finance personnel for determining the impacts to the organization if these are lost or damaged. This can be a tedious process, and one that should be carried out by a team of qualified professionals. Also, managers have limited budgets and must prioritize their spending according to the severity and likelihood of threat risks.

The security assessment and planning functions of management may draw from guidelines, standards, and best practices. For example, the Federal Information Processing Standard (FIPS) is necessary for government systems, but may also serve as a process and criteria for commercial enterprises. As part of the E-Government Act of 2002 (Public Law 107-347), the FIPS-200 became "the second of the mandatory security standards, specifies minimum security requirements for information and information systems supporting the executive agencies of the federal government and risk-based processes for selecting the security controls necessary to satisfy the minimum security requirements" [16]. The specification defines a useful formula as follows: A security category (SC) of an information system = {(confidentiality, impact), (integrity, impact), (availability, impact)}, where the acceptable values for potential impact are low, moderate, or high. This formula hints at ways managers can categorize their information and assets and the risks to them regarding their **CIA**: ***confidentiality, integrity, and availability***.

FIPS-200 subsumes FIPS-199 (Standards for Security Categorization of Federal Information and Information Systems) for risk-based processes in selecting security controls necessary to satisfy the minimum security requirements and requires assessment and planning involving activities related to (1) access controls, (2) awareness and training, (3) audit and accountability, (4) certification, accreditation, and security assessments, (5) configuration management, (6) contingency planning, (7) identification and authentication, (8) incident response, (9) security maintenance, (10) media protection, (11) security planning, (12) personnel security, (13) risk assessment, (14) systems and services acquisition, (15) system and communications protection, and (16) system and information integrity.

Rather than trying to "reinvent the wheel," using standards such as these for guidelines may help save time and money, as well as promote the development, implementation, and operation of more secure information systems, establishing reasonable levels of due diligence for information security, and facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems that meet minimum security requirements.

1.2.1 Financial Evaluations

It is typically an important part of a manager's job to handle budgets and develop financial justifications. In security, we are interested in assessments of the value of assets and the financial impacts from losses. We use economic forecasting formulas such as annualized loss expectancy, payback period on repurchases, and others to determine the financial impacts of security incidents. However, financial assessments are best done in conjunction with the accounting and finance departments in the organization rather than having line or security managers try to figure the value of equipment and software on their own. This is because capital assets may be in various stages of depreciation or may have different net present valuations on the books than those formulated by managers.

If managers make written financial declarations, this might actually become a problem for the company because financial audits by the Internal Revenue Service (IRS), insurance companies, due diligence mergers and acquisition (M&A) teams, lending institutions, or

the company's auditing firm may turn up discrepancies that might create difficulties for the company if there is a dispute down the road. We are not suggesting that managers should not use financial formulas to try to predict exposure and loss—after all, this is part of managing one's budget—but we are suggesting that managers should not make financial declarations involving asset valuation without the active and expressed involvement of the finance and accounting departments.

Because managers are often not involved in the economic transactions undertaken by the organization, another important reason managers need to involve the finance and accounting departments in assessing asset value and making financial decisions is because managers sometimes accidentally inflate the value of assets in their reporting [17–19], and these financial reports may be "rolled up" into the financial collateral of the company [20, 21]. This issue is particularly noteworthy in public companies, which fall under the Sarbanes–Oxley Act of 2002 [22] that requires that company officers (Chief Executive Officer and Chief Financial Officer) to certify and approve the integrity of their company financial reports at the risk of their own personal liabilities.

All in all, the accuracy of asset valuations such as in risk assessments is crucially important—as important as any other security measure. With the help of the finance department, financial projections and assessments act as guidelines for managers to prioritize their efforts and budget expenditures. Managers should be in a position to provide the qualitative assessments of risks and the quantitative values of new and replacement software and equipment to the finance department for determining value—but again, we emphasize that managers should not proclaim financial valuations any more than they should act as legal counsel regarding legal matters.

1.2.2 Attacks, Monitoring, and Recovery

Attacks from the outside tend to follow a predictable pattern [23]. Outsider attacks may begin with *foot printing*—a technique using technologies to determine the network infrastructure of a target such as what internet protocol (IP) addresses the company uses. They then *scan* this infrastructure to find networked services (ports), protocols, and software that the company provides, supports, and uses—as well as versions and security patch and revision levels of software—so the attacker may know what vulnerabilities can be exploited. They then use *enumeration* to find what connections and parameters specific services allow. Once this is known, they try to *infiltrate or penetrate* the targeted system, and then the attacker strives to cover his or her tracks, which means removing as much evidence as possible that the attack occurred. In the case that an attack succeeds, the management process also follows a predictable pattern of discovery, recovery, forensic analysis, preserving evidence, incident reporting, and creating a feedback loop.

In most cases, the attack process is monitored at some point [1]. Intrusion detection systems (IDS) may be computer host-based (HIDS) or network-based (NIDS). Host-based IDS such as the OSSEC (http://www.ossec.net/main) monitor a computer system by analyzing log files, checking the integrity of files to ensure they have not been tampered with, providing automated policy monitoring, and checking for illicit tools used to escalate an unauthorized user's privileges (called rootkit detection). Common network-based IDS

such as Wireshark and SNORT, or commercial intrusion detection and prevention applications such as Radware, Panoscopia, or Intelligent Access Systems (AIS), can be installed on host systems or on routers or gateways to monitor protocols and ports, bandwidth utilization, packet contents, and utilizations that indicate potential threats.

In Focus

Statistical anomaly–based IDS determine normal network activity such as average bandwidth used at a given time and then alert an administrator when anomalies are noted (typically using a form of regression for this). Signature-based IDS are configured with and receive updates to a "signature" database (of threats). Activity is compared with these attack patterns (signatures). Important here are two concepts—false positives and false negatives. False positives occur when an IDS falsely determines some activity as "bad" and generates an alert or blocks legitimate access, when actually, it is "legitimate" activity. Statistical (anomaly) IDS is more prone to these errors than signature-based IDS. False negatives occur when the IDS fail to detect an attack. Signature IDS are more prone to false positive attacks, whereas anomaly detection is more prone to false negatives because there is no previously established attack profile (often called a first-day attack). Digital forensics is related to this and includes investigating and preserving the evidence gathered by IDS. Log files require Digital Signature (a Message Digest) to show that data have not been tampered with. A "chain of custody" must be established and proved if the evidence is to be presented in court.

How managers respond to attacks will likely include a multi-phased strategy that involves asking questions such as (1) What should managers do about identifying the attacker(s)? (2) How should they try to contain or quarantine the attack? (3) How should they eradicate an infection? (4) How do they try to recover and continue critical business operations? (5) How do they recover from an attack? and (6) What should they do to determine the lessons learned and how they should apply them to prevent similar attacks in the future?

If the organization decides to pursue legal action against an attacker, evidence must be gathered and preserved in a way admissible in a court of law. This may include retaining log files and other electronic and non-electronic records, establishing a chain of custody of these materials and proving they were not altered along the way, explaining the methods used in the investigation of the attack, and describing how the manager and/or administrator determined that a security violation was in the process of occurring or had occurred. In anticipation of this, it is important for managers to maintain records related to incidents, and the process involves multiple people including the legal department. Policies, rules, and procedures need to have been established ahead of time on how various incidents should be handled and what to do about reporting them, and managers and all personnel involved in handling security incidents need to be knowledgeable of these.

1.2.3 Reasons Why "They" Attack "Us"

Schultz [24] provided an overview of theories that try to explain why people attempt to breach security. Knowing these reasons helps managers with determining what actions to

take in response. There are many different conceptual models for why people carry out attacks. One such model used by law enforcement is called the *CMO model*. The CMO model postulates that in order to commit an attack, the perpetrator must first have the capability to commit the attack such as having the skills and technologies to do so. However, having only the capability is insufficient. A perpetrator must also have a motive for the attack. Typical motives for attacks include greed and revenge. Given the capability and one or more motives, the attacker must also have an opportunity to commit the attack for it to succeed [25]. Opportunity is enhanced by factors such as remote access to target systems. However, simply having capabilities, motives, and opportunities may not be enough. To get at weaknesses that can be exploited, the attacker may need to collude with others, including those on the inside [1].

As noted by Schultz [24], Parker [26] presented an attack model similar to the CMO but with slightly different factors that included whether the attacker had sufficient skills, knowledge, and resources to succeed, and these accounted for motives ranging from computer crimes committed by insiders to outsider attacks. Tuglular and Spafford [13] took issue with the Parker model and suggested that a single model was not adequate in describing such broad outcomes. Instead, Tuglular and Spafford focused on insider attacks and argued that for an insider attack to succeed, he or she must first be able to use a given computer system with the level of authority granted to the insider, and then he or she must be able to perform some activity to harm the functions that support the organization's mission.

Building on the CMO model, Gudaitis [27] developed three-dimensional profiling (3DP). This approach focused on insider attacks and prescribed an organizationally based method for prevention. The utility of this model was twofold in that it (1) assessed an incident or attack using profiling in addition to the usual technical tools and (2) provided organizations with a way to evaluate and enhance their security processes and procedures from a human perspective as a preventive measure [1].

Some research models have formulated explanations of simple misuse of systems. Misuse in this research literature is defined as a violation of the policies established in an organization to prevent corruption of information or more malevolent actions. According to Schultz [24], insider misuse is a cumulative function of personal and organizational factors such as personality, motivation, knowledge, abilities, rights, restrictions, obligations, authority, and responsibility.

Another approach to explaining security violations has been termed a *psychodynamic driven model* as described by Shaw, Ruby, and Post [28]. This profiled the psychological makeup of convicted cyber criminals, and then categorized them as introverts and depressed people. Nevertheless, this model was limited in its explanatory power because (1) the results were drawn from convicted criminals after the fact; (2) the study was based on a small subset from a convenience (not a random) sample (the perpetrators who were caught, arrested, and convicted, as well as those who agreed to participate in the study); (3) the model included only outside attackers; and (4) the results were based exclusively on the measurement of psychological factors, even though other factors (e.g., organizational and socioeconomic factors) may have been involved [1].

Collins [29] studied the relationship between social context cues and uninhibited or abusive verbal or written behavior in online communication. This model establishes a predictive connection between the absence of social context cues and the presence of uninhibited (i.e., flaming and inappropriate language) verbal behavior, and provides some interesting insights into cyber harassment and defamation against companies and company managers. This was supported in a study by Workman [30] on factors that translate between those who cyber harass others and those who conduct cyber attacks against companies.

Finally, Morahan-Martin [31] described the general use of computers and computer behaviors across demographics, specifically focusing on gender differences. This model posited cultural and linguistic aspects of computer behavior as they relate to computer competency and Internet competency. It incorporated the notion that computer self-efficacy (competency) not only predicts computer-related behavior, but it also makes predictions about behavior online, and thus the model extends deviant or unethical computer behavior to adversarial and status-enhancing behaviors online, as demonstrated by the use of certain rhetoric [1].

These conceptual models have provided a good start in helping managers with determining meaningful measures and countermeasures to help organizations reduce the frequency and damage resulting from insider attacks. However, most do not adequately facilitate practical ways of detection, let alone prediction of insider attacks. Detection capability is desirable, but unfortunately it comes after the damage has been done. Given the potential damage that can result from insider attacks, detecting insider attacks is very important. Without understanding and control of the human element, technology alone cannot provide the level of information security needed by organizations today [24].

So what should managers do? In the chapters that follow, we will provide some important guidance regarding what managers should do, and in particular, we will give some insights into predicting current and impending attacks so managers can intervene sooner and more effectively. This is the touchstone of our textbook.

The textbook chapters that follow will stage each learning domain. First, we will present the organization context in which managers operate. We will then provide a section on technology to orient managers toward the next section on how to protect resources, technological systems, and infrastructure. We will conclude with a broad view of what managers are doing to predict attacks and what they are doing to predict attacks and ways to take appropriate actions.

Let's get started!

References

1. Schultz, E. E., & Spafford, E. H. (1999). Intrusion detection: How to utilize a still immature technology. In M. Krause and H. F. Tipton (Eds.), *Handbook of information security management*. New York, NY: Auerbach.

2. Workman, M. (2008). Fear commerce: Inflationary effects of global security initiatives. *Information Security Journal: A Global Perspective, 17*, 124–131.
3. Hernandez, H. (2010). Cyber crime wave—Who pays? *Market Times, 12*, 12–23.
4. O'Connell, K. (2008, January). Cyber fraud and online bullying affect 44% of small Irish businesses. *Internet Business Law*. Retrieved October 10, 2011, from http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=1954
5. Brenner S. W. (2010). Cybercrime and the U.S. criminal justice system. In H. Bidgoli (Ed.), *The handbook of technology management* (pp. 693–703). Hoboken, NJ: John Wiley & Sons.
6. Beadle, J. (2010). Corporate law and legal counsel: A mutually dependent relation. *The Legal Brief, 15*, 19–27.
7. Borrull, A. L., & Oppenheim, C. (2004). Legal aspects of the Web. In B. Cronin (Ed), *Annual Review of Information Science and Technology, 38* (pp. 483–548). Medford, NJ: Information Today.
8. Bartels, A. (2006, November). Global IT spending and investment forecast, 2006–2007. *Forrester Research,* pp. 4–31.
9. Bragdon, C. R. (2008). *Transportation security*. Burlington, MA: Elsevier/Butterworth-Heinemann.
10. ISOO. (2004). *The report on cost estimates for security classification activities for 2003 from the Information Security Oversight Office (ISOO)*. Washington, DC: National Archives and Records Administration.
11. Straub, D. W., Goodman, S., & Baskerville, R. L. (2008). *Information security: Policy, processes, and practices*. Armonk, NY: Sharpe Books.
12. Cisco. (2009). *2009 Annual security report*. Retrieved March 19, 2011, from http://cisco.com/en/US/prod/vpndevc/annual_security_report.html
13. Tuglular, T., & Spafford, E. H. (1997). *A framework for characterization of insider computer misuse*. Unpublished colloquium presentation, Purdue University.
14. Rothfeder, J. (1996). Hacked! Are your company's files safe? *PC World, 14,* 70–74.
15. Davis, K., & Newstrom, J. W. (1989). *Human behavior at work*. New York, NY: McGraw-Hill.
16. NIST. (2006). *Minimum security requirements for federal information and information systems.* Gaithersburg, MD: FIPS Pub 200. Retrieved March 17, 2011, from http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf
17. Aberdeen Group. (2002). *Technology forecasting consortium: 2002 user buying intentions*. Boston, MA: Aberdeen and Associates.
18. Bagozzi, R. P., Davis, F. D., & Warshaw, P. R. (1992). Development and test of a theory of technology learning and usage. *Human Relations, 45*, 659–686.
19. Morris, H. (2002, June). Analytic applications market forecast and analysis: 2001–2005, *IDC Report,* pp. 17–21.
20. Carroll, J. (2003). *Take the stress away*. Retrieved March 10, 2011, from http://proquest.umi.com/pdqweb?index=4&sid=srchmode=1&vinst=PROD&fmt=3&star

21. Venkatesh, V., Morris, M. G., & Ackerman P. L. (2000). A longitudinal field investigation of gender differences in individual technology adoption decision-making processes. *Organizational Behavior and Human Decision Processes, 83*, 33–60.
22. Sarbanes–Oxley Act of 2002, Pub.L. No. 107–204 (July 30, 2002); 116 Stat. 745 (2002).
23. Thomas, T. (2004). *Network security*. Indianapolis, IN: Cisco Press.
24. Schultz, E. E. (2002). A framework for understanding and predicting insider attacks, *Computers & Security, 21*, 526–531.
25. Bugge, B. K. (1996). *Principles of law in investigations*. Scranton, PA: Harcourt.
26. Parker, D. B. (1998). *Fighting computer crime: A new framework for protecting information*. New York, NY: John Wiley, NY: Sons.
27. Gudaitis, T. M. (1999). The missing link in information security: Three dimensional profiling. *Cyber Psychology and Behavior, 1*, 4–14.
28. Shaw, E. D., Ruby, K. G., & Post, J. M. (1998). The insider threat to information systems. *Security Awareness Bulletin, 2*, 27–46.
29. Collins, M. (1992). *Flaming: The relationship between social context cues and uninhibited verbal behavior in computer-mediated communication*. Retrieved March 17, 2011, from http://star.ucc.nau.edu/~mauri/papers/flames.html
30. Workman, M. (2010). A behaviorist perspective on corporate harassment online: Validation of a theoretical model of psychological motives. *Computers & Security, 29*, 831–839.
31. Morahan-Martin, J. (1998). Women and girls last: Females and the Internet. *Proceedings of the International Conference Research and Information Systems, Bristol: UK: IRISS'98*, 25–27.