A Framework for Information Security Management Based on Guiding Standards: A United States Perspective

Janice C. Sipior and Burke T. Ward
Villanova University, Villanova, PA, USA

janice.sipior@villanova.edu burke.ward@villanova.edu

Abstract

Despite government oversight, consumers continue to be concerned about the security of personal information used by corporations. Consumer concerns give rise to the necessity for corporations to manage information security. Navigating the multitude of existing security standards, including dedicated standards for information security and frameworks for controlling the implementation of information technology, presents a challenge to organizations. In response, we propose our ISM framework which considers global, national, organizational, and employee standards to guide ISM. We contend that a strategic approach to ISM will enable a focus on managing information as a key resource in global competition. This framework is intended to promote a cohesive approach which considers a process view of information within the context of the entire organizational operational environment. This framework can be used by international, national, and regional corporations to formulate, implement, enforce, and audit information security policies and practices.

Keywords: information security, security standards, security policy, strategic information security management, IT management.

Introduction

Information is widely exchanged in business transactions among employees, partners, customers, and other stakeholders. The technological capabilities of the internet enable a wealth of information to be gathered, combined, and disseminated, with relative ease. Despite government oversight, consumers continue to be concerned about the security of personal information used by corporations. Consumer concerns give rise to the necessity for corporations to manage information security. Organizations have a responsibility to protect consumer and organizational proprietary information while ensuring compliance with laws and regulations (Sipior, 2007). However, internet use has brought about an escalation of concerns including consumer confidence in online business activities, threats to data integrity, legal liability, and risk of financial loss. These, and other concerns, result in ever-increasing threats to organizations by terrorists, hackers, and even employees.

Information security management (ISM) may be defined as "a systematic approach to encompassing people, processes, and Information Technology (IT) systems that safeguards critical systems and information, protecting them from internal and external threats" (Barlas,

Queen, Radowitz, Shillam, & Williams, 2007). Research on ISM generally addresses two areas, the technical computer security and non-technical security management, while some researchers span both areas (Baskerville & Siponen, 2002). Within the technical computer security literature, security policy is used as a synonym for overall security architecture of operating systems; while non-technical security management literature addresses the access control rules for a computer system. The focus of this paper is primarily on non-technical security management.

ISM is increasingly important within organizations, becoming a strategic imperative as security threats continue to escalate (Okin, 2006). Security and privacy is among the top ten IT management concerns, according to a 2005 survey of executive IT managers (SIM, 2006). For Certified Public Accountants, ISM has topped the list of the American Institute of Certified Public Accountants' (AICPA) annual top technology initiatives, expected to have the greatest impact in the coming year, for the past five years (Barlas et al., 2007). Proper management of information security requires a formal structure and resources (Mogul, 2002). The absence of a well-defined information security policy is currently regarded as the most serious problem with security in organizations today (Biegelman & Bartow, 2006). The vice president of security at Openheimer Funds recognizes that "senior managers need to assume an active role in addressing the security on their systems" (McCarthy, 2003, p.35).

Navigating the multitude of existing security standards, including dedicated standards for information security and frameworks for controlling the implementation of IT, presents a challenge to organizations. Adding to the challenge is the increase in activities of terrorist groups and organized criminal syndicates. A strategic approach to ISM will promote a focus on proper management of information as a key resource in global competition. In response, we propose our ISM framework which considers global, national, organizational, and employee standards to guide the management of information security. This framework can be used by international, national, and regional corporations to guide the formulation, implementation, enforcement, and auditing information security policies and practices.

The Information Security Management Framework

The ISM framework considers global, national, organizational, and employee standards to guide ISM. This framework is intended to promote a cohesive approach which considers a process view of information within the context of the entire organizational operational environment. The four levels of guiding standards for ISM are presented in Figure 1 and are discussed in the following sections.

We caution corporations, using this guiding framework, that the relations among the four levels of information security depicted in Figure 1 are complicated. For example, at the international level, standards may very by country. Similarly, at the national level, various government agencies may have possibly conflicting standards. Organizational standards may not be in line with those of business partners. Employee practices may be influenced by professional rules of conduct in addition to organizational policy.

Figure 1: The Information Security Management Framework based on Guiding Standards

Global Standard for Information Security Management

The most widely accepted global standard for ISM across industries and geography is the International Standards Organization / International Electrotechnical Commission (ISO / IEC) Code of Practice, document number 27002 (Biegelman & Bartow, 2006; Langley, 2006; Rasmussen, 2005). ISO / IEC 27002:2005 provides a commonly accepted security architecture framework of guidelines and general principles for developing organizational security standards and effective security management practices. The standards address people, processes and IT systems to assist in identifying, quantifying and managing threats to information.

ISO / IEC 27002:2005 was originally written by the United Kingdom (U.K.) Government's Department of Trade and Industry (DTI) and published as BS 7799 by the British Standards Institute (BSI) in 1995 (Langley, 2006). BS 7799 was eventually internationalized and adopted by ISO in 2000, as ISO/IEC 17799, "Information technology - Security techniques - Code of practice for information security management," after several revisions. ISO/IEC 17799 was most recently revised in June 2005 and subsequently renumbered to ISO/IEC 27002 in July 2007 to align with the ISO/IEC 27000 series standards. This series is intended to provide further guidance for ISM system requirements, risk management, metrics and measurement, and implementation (Rasmussen, 2005).

Global standards must also consider the increasing activities of international terrorist groups and organized criminal syndicates (Trim, 2007). Terrorists and criminals are forming alliances and using increasingly sophisticated technologies to devise new activities threatening to IT. Thus, governmental transnational intelligence sources should be consulted by organizations to remain apprised of emerging concerns (Trim, 2007). Information security is a concern for all organizations across the world, necessitating the sharing of global intelligence. A balance between security and privacy, that is acceptable to the majority of the community worldwide, must be found (Berinato, 2007).

National Standards for Information Security Management

At the national level, governments create information security standards and regulations. Within the United States (U.S.) for example, there is no single authority to reference for organizational ISM. The lack of a strong enforcement mechanism to protect personal information is one of the primary criticisms of U.S. privacy practices (Fredericks, 2005). However, several laws are directed toward specific industry sectors. Organizations in the public sector and the regulated industries are required to demonstrate proper ISM procedures and controls associated with storage, backup, encryption, security, and protection of confidential data to avoid penalties for non-compliance (Mohamed, 2007).

Several federal laws are directed toward specific industry sectors to increase corporate responsibility in protecting consumer privacy and accountability for the substance of their financial reports. The current regulatory environment within the United States has made ISM a strategic necessity. For example, the Financial Services Modernization Act of 1999, also known as the Gramm-Leach Bliley Act (GLBA), requires financial institutions to maintain the privacy of electronically stored customer information through security controls for data integrity and for identifying with whom this information is shared (Federal Trade Commission, n. d.). The Health Insurance Portability and Accountability Act (HIPAA) of 1995 is intended to protect electronic health information (Hewitt, 2004). Standards for policies and procedures to limit unauthorized access to medical information were set in the Security Rule, published February 2003 (Gue, 2003). Section 404 of the Public Company Accounting Reform and Investor Protection Act of 2002, or Sarbanes-Oxley, requires publicly held companies to annually evaluate their financial reporting controls and procedures (AICPA, 2004). Although information security is not explicitly addressed, compliance may be incomplete without adequate security controls. Another example of federal legislation is the Family Educational Rights and Privacy Act (FERPA), which protects the privacy of student education records (Family Educational Rights, n.d.). Controls are required to prohibit unauthorized access and to control the sharing of the information.

Similar to the necessity to consider the increasing activities of international terrorist groups and organized criminal syndicates for global standards, national standards must also take into account the actions of such perpetrators. In the U.S. for example, the number of computer intrusions or attacks is rising. The U.S. Department of Homeland Security reported a 152% increase in such activities from fiscal year 2006 to 2007, from a recorded 24,000 reports of attempted breaches on private and federal systems to 37,000 (Montgomery, 2007). Security concerns may be specific to countries, regions, and industries, again calling for the need to share intelligence and security information across these units. However, such information sharing requires a balance between privacy interests and national security.

Organizational Standards for Information Security Management

Organizations must formulate their own practical and effective ISM in support of international standards, government regulations, and business goals (Biegelman & Bartow, 2006). Organizations tend to focus on technical solutions (Rasmussen, 2005). A disproportionate focus on technical security countermeasures, with less consideration for management controls, can contribute to the continuation of security concerns (D'Arcy & Hovav, 2007). However, in developing an organizational information security policy (ISM), information security should be linked to a business necessity. For example, The Vanguard Group, Inc. vigilantly guards the privacy of clients' social security numbers which are critical to the operations of the world's only virtual investment company (McGee, 2006). Customer concerns are an important factor to ISM practice (Ezingeard & Bowen-Schrire, 2007). A balance between adequate data protection and reasonable, confidential use of information must be made (Fredericks, 2005). This balance extends to the use of out-

sourcing. If, for example, an outsourcer in a distant low-wage country is used to maintain stored information, it may be more difficult to control security and privacy.

Information Security Management by Employees

Ultimately, the policies and procedures of the ISM are carried out by employees. Most security failures are related to errors caused by employees ("Security: Protect information first," 2007). For example, strategic level employees may poorly design an information security policy (ISP); tactical and operation level employees may misinterpret a poorly designed policy or bypass policy requirements. Organizations recognize that their employees must protect information (Fredericks, 2005), as privacy breaches by employees can be an unwitting avenue to noncompliance. The biggest security threat results from malicious or negligent employees or from faulty controls and oversight (Swartz, 2007). Thus, it is in the interest of the organization to hire employees whose individual privacy concerns, perceptions, and actions are congruent with professional values. As mentioned, outsourcers may not employ the same controls and oversight as those applied by employees of the corporation itself. The concern about the use of outsourcing, mentioned in the discussion of organizational standards, extends to employee practices as well. Recognizing the consequences of the ISM on employees and the organization is critical (Mogul, 2002). Security practices of employees should be placed within the more holistic security management decision-making context (Trim, 2007).

Integrating the ISM Framework within Organizations

It is a strategic imperative that the security of information be maintained. Table 1 presents our recommended approaches to integrate the ISM framework within organizations. Our first recommendation is based on the recommendation of Dhillon (1997) to set an information security vision and strategy. We extend this recommendation by proposing that organizations take a comprehensive approach to ISM through the incorporation of the ISM framework into the overall strategic plan. Top management support is more likely to be secured if ISM fits with corporate strategy and culture (Purtell, 2007). The information vision and strategy must be disseminated throughout the organization. Poor communication and lack of top management support can result in ISM designed for operational convenience or a check-the-box approach to compliance with standards and regulations (Ezingeard & Bowen-Schrire, 2007). Formalization of ISM, monitoring, and follow-up evaluation can improve the probability of successful on-going ISM. To fully integrate the framework, the depth of specific controls for the organizational environment must be devised within the security infrastructure (Rasmussen, 2005).

Table 1: Approaches to Integrate the ISM Framework within Organizations
Incorporate the holistic ISM framework into the overall strategic plan
Secure executive support
Disseminate he information security vision and strategy throughout the organization
Formalize ISM, monitor, and undertake a follow-up evaluation
Include dual lines of reporting for the Chief Security Officer (CSO) to both the Chief Executive Officer (CEO) and the Chief Information Officer (CIO)
Promote effective communication between the CEO and the CSO

Formulate a formal Information Security Policy (ISP)
Create a pervasive security culture • Convey the strategic value of information security throughout the organization • Hire and cultivate trustworthy employees whose values are congruent with those of the overall organizational ISM strategy and practices • Train employees in security awareness and appropriate security practices • Internally promote security awareness • Encourage security practices through scenario analysis and simulation exercises, reinforced with team-building • Cultivate security champions
Create mechanisms for continuous improvement for ISM

Responsibility for the ISM Framework

The Chief Executive Officer (CEO) and top managers responsible for ISM must align their information security vision with the framework to comprehensively consider the four levels of guiding standards. This may present a challenge as the role of the top manager responsible for information security continues to undergo change. A recent trend, especially in large organizations, was to separate the responsibility for security from the Chief Information Officer (CIO) to the Chief Security Officer (CSO) (Berinato, 2007). The initial role of the CSO was to assure no unauthorized access to IT resources. The responsibilities of this role have increased from overseeing tactical controls to a strategic perspective of aligning security and business objectives. As national security and privacy laws were enacted, the CSO assumed an oversight role to assure compliance with regulatory requirements. Responsibility for physical security converged with that of information security (Berinato, 2007). As the responsibilities of the CSO increased, the trend was to instill more decision making authority and shift reporting to functions external to IT such as the legal department, the risk department, and directly to the Chief Executive Officer (CEO) (Berinato, 2007). However, an emergent trend of security executives again reporting to the IT executive, such as the CIO or Chief Technology Office (CTO) may be occurring (Berinato, 2007). Alternatively, dual lines of reporting, including a direct link to both the CEO for strategic alignment and the IT executive for a pragmatic connection to operations, promotes the opportunity for greater integration of information management considerations. Regardless of the reporting structure, a locus of responsibility for ISM will provide a clear authority for ISM (Ezingeard & Bowen-Schrire, 2007; Purtell, 2007). Effective communication between the IT executive responsible for ISM and the Chief Executive Officer (CEO) is necessary to achieve integration and responsibility. Further, members of the board of directors should be engaged in ISM management issues as well (Ezingeard & Bowen-Schrire, 2007).

Organizational Information Security Policy

A formal written Information Security Policy (ISP) should be formulated by addressing concerns at each of the levels in the ISM framework. An ISP formalizes organizational principles and guidelines for information security. Developing or adopting a comprehensive ISP which focuses on procedures and implementation considerations has empirically been found to be an effective managerial measure to increase security in organizations (Hong, Chi, Chao, & Tang, 2007). Classifying security concerns according to high-level and low-level ISP requirements aids in the

identification of who within the organization is responsible for creating or contributing to the policy (Baskerville & Siponen, 2002). The policy statements should be translated into acceptable employee security practices. Although our focus in this paper concerns security management, the ISP should address not only managerial, but technical considerations, as well.

Creating a Pervasive Security Culture

The strategic value of information security must be conveyed throughout the organization. The revelation that insider employees, rather than outside hackers, increasingly are the culprits in security incidences can result from the deployment of tools to monitor and investigate anomalies associated with IT resources (Berinato, 2007). A substantial percentage of information security breaches result from the actions of legitimate users (D'Arcy & Hovav, 2007). In 2006, 51% of respondents to an annual security survey identified employees, both current and former, and 54% identified hackers as the source of security incidences (Berinato, 2007). In 2007, these percentages reversed and widened to 69% and 41%, respectively. These results reveal the critical necessity to hire and cultivate trustworthy employees whose values are congruent with those of their profession and with those of the overall organizational ISM strategy and practices. Values are beliefs about appropriate behaviors and outcomes (Rokeach, 1978). As individuals identify with and adopt a set of values they serve as benchmarks to guide actions, form attitudes, and make evaluations (Vance, 2000).

To create a pervasive security culture, the value of information security to the corporation must be widely communicated. To reinforce behavioral change, various approaches may be undertaken. Employees should be trained in security awareness and appropriate security practices. Awareness can be further advanced through internal promotional techniques, such as cascading voicemail and email campaigns from senior executives to their subordinates (Cisco Systems, 2006). Scenario analysis and simulation exercises can be utilized, in conjunction with team-building, to encourage employees to perform new security practices (Trim, 2007). The CSO or other IT executives responsible for ISM can develop relationships and cultivate security champions (Cisco Systems, 2006) to disseminate important communications, demonstrate acceptable practices, and maintain momentum regarding the criticality of appropriate security measures throughout the organization.

Global corporations cannot simply assume that the same security culture will be present in the various countries in which they operate. A Silicon Valley startup company, for example, disabled connectivity to internet and USB ports in their chip application development centers in China to protect proprietary information (Holstein, 2007). The approaches to integrating the ISM framework within organizations should be applied at all locations. Additional efforts should be undertaken such as limiting information availability to small disparate segments, enforcing codes of conduct for employees, creating a climate in which employees are informed of capabilities for monitoring and tracking the flow of information, reinforcing corporate and personal agreements annually, and creating legal and compliance departments locally (Holstein, 2007).

Continuous Improvement for ISM

To promote effective ISM, organizations must continue to be informed about environmental changes and improvements in approaches. Continuous improvements, whether in response to environmental incidences or internal reviews, are important to ensure the adequate protection of information resources (Ezingeard & Bowen-Schrire, 2007). To assess the adequacy of current practices, measuring and reporting of risks, control issues, and vulnerabilities are necessary (Purtell, 2007). In designing appropriate measures, the ISM framework integrated into the overall strategic plan should be referenced so that the metrics conform with the vision and requirements for the organization.

Conclusion

Information is a key resource in global competition. Organizations spent a reported 15% of the IT 2006 budget on information security and increased the rate of security staff hiring, but did not realize improvements in enterprise security, according to a 2006 annual security survey (Berinato, 2007). In 2002, 36% of the respondents to the same annual information security survey reported having experienced zero security incidences, while this rate dropped to 22% reporting no security incidences in 2007 (Berinato, 2007). It appears that resources devoted to building an ISM infrastructure have increased, resulting in an increased awareness of information security. Although awareness is higher, organizations do not have an understanding of the type of security incident and the primary method used to breach security. The percentage of respondents who reported not knowing the number and nature of security incidences rose from 29% in 2006 to 40% in 2007. In response to the necessity to realize improvements in enterprise security, we recommend that corporations take a comprehensive approach to ISM by incorporating the ISM framework into the overall strategic plan.

References

AICPA. (9 June 2004). *Summary of Sarbanes-Oxley Act of 2002*. Retrieved March 15, 2008, from http://www.aicpa.org/info/sarbanes_oxley_summary.htm.

Barlas, S., Queen, R., Radowitz, R., Shillam, P., & Williams, K. (2007). Top 10 technology concerns. *Strategic Finance, 88*(10), 21.

Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management, 15*(5/6), 337-46.

Berinato, S. (2007, August). The end of innocence. *CIO Magazine*. Retrieved March 15, 2008, from http://www.cio.com/article/133600/

Biegelman, M. T., & Bartow, J. T. (2006). Information security and fraud. In M. T. Biegelman & J. T. Bartow, *Executive Roadmap to Fraud Prevention and Internal Controls: Creating a Culture of Compliance* (Chapter 10, pp.121-127). Hoboken, NJ: John Wiley & Sons.

Cisco Systems. (2006). *Security at center stage: The evolving role of the Chief Security Officer and 5 secrets to CSO success*. Retrieved March 15, 2008 from http://www.csoonline.com/whitepapers/Cisco_Oct_FINAL.pdf.

D'Arcy, J., & Hovav, A. (2007). Deterring internal information systems misuse. *Communications of the ACM, 50*(10), 113-117.

Dhillon, G. (1997). *Managing information systems security*. London: Macmillan Press.

Ezingeard, J.-N., & Bowen-Schrire, M.. (2007). Triggers of change in information security management practices. *Journal of General Management, 32*(4), 53-72.

Family Educational Rights and Privacy Act (FERPA). (n. d.).. Retrieved March 15, 2008 from US Department of Education http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

Federal Trade Commission. (n. d.). *Financial privacy: The Gramm-Leach Bliley Act*. Retrieved March 15, 2008 from http://www.ftc.gov/privacy/glbact/

Fredericks, P. (2005). Security and privacy principles toward a universal set of principles for these universal business concerns. *Forsythe*. Retrieved March 15, 2008 from www.forsythe.com.

Gue, D. (2003). The HIPAA Security Rule (NPRM): Overview. *HIPAAdvisory*. Retrieved March 15, 2008 from http://www.hipaadvisory.com/regs/securityoverview.htm

Hewitt, C. (2004). HIPAA/Secure: Security Q/A. *HIPAAdvisory*. Retrieved March 15, 2008 from http://www.hipaadvisory.com/action/secureqa/secure.htm.

Holstein, W. J. (2007). Protecting the company jewels in an unprotected country. *Research Technology Management, 50*(6), 14-16.

Hong, K.-S., Chi, Y.-P., Chao, L. R., & Tang, J.-H. (2007). An empirical study of information security policy on information security elevation in Taiwan. *Information Management and Computer Security, 14*(2), pages unavailable.

International Organization for Standardization. (2005). Code of practice for information security management. *ISO/IEC* 17799:2005. Retrieved March 15, 2008 from http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html.

Langley, N. (2006, November 7). BS 7799 can open door to information security work. *Computer Weekly*, 56.

McCarthy, L. (2003). *IT security: Risking the corporation*. New Jersey: Prentice Hall PTR.

McGee, K. (February 7, 2006). *IT leaders' next big decisions*. Group Vice President and Research Fellow at Gartner Inc., Evening Speaker, Society for Information Management, Philadelphia Chapter meeting.

Mogul, R. (2002). *Danger within –Protecting your company from internal security attacks*. Gartner Group. Retrieved March 15, 2008 from http://www.csoonline.com/analyst/report400.html.

Mohamed, A. (2007, April 24). The route to compliance. *Computer Weekly*, pages unavailable.

Montgomery, D. (2007, November 26). Hacker threat to U.S. rising: Civilian, military dependence on computers makes security vital. *Sacramento Bee*, p. A1. Retrieved March 15, 2008 from http://www.sacbee.com/111/story/520067.html

Okin, S. (2006, January/February). Information security and the board: Keeping risk out and letting business in. *SIM News*. 1-3. Retrieved March 15, 2008 from http://www.simnet.org/Content/NavigationMenu/Resources/SIM_News_-_January_February_2006/Features5/Features.htm.

Purtell, T. (2007). A new view on IT risk. *Risk Management, 54*(10), 28.

Rasmussen, M. (2005). Revised ISO 17799 boosts information security management relevance. *Forrester® Analyst Reports*. Retrieved March 15, 2008 from http://www.csoonline.com/analyst/report3730.html.

Rokeach, M. (1978). *Psychology and applied ethics*. New Jersey: Lawrence Erlbaum Associates.

Security: Protect information first. (2007). *American Bankers Association Banking Journal, 99*(9), 54-55.

SIM (Society for Information Management). (2006, January/February). Security: Addressing a top concern for SIM members. *SIM News*. Retrieved March 15, 2008 from http://www.simnet.org/Content/NavigationMenu/Resources/SIM_News_-_January_February_2006/Features5/Features.htm.

Sipior, J. C. (2007). Editorial preface: Ethically responsible organizational privacy protection. *Information Resources Management Journal, 20* (3) i-iii.

Swartz, N. (May/June 2007). Protecting information from insiders. *Information Management Journal*. *41*(3), 20-24.

Trim, P. R. J. (2007). Managing computer security issues: Preventing and limiting future threats and disasters. *Disaster Prevention and Management, 14*(4).

Vance, D. (2000). *Effects of corporate information privacy policy on employment opportunity attractiveness*. Dissertation. Southern Illinois University, Carbondale, IL.

Biographies

Janice C. Sipior is a Professor in the Accounting & Information Systems Department at Villanova University in Pennsylvania USA. She was a Visiting Professor at Moscow State Linguistic University in Russia and University of Warsaw in Poland. She is Chair of the Association for Computing Machinery - Special Interest Group on Management Information Systems (ACM-SIGMIS), represents ACM on the ACM/Association for Information Systems (ACM/AIS) Task Force for IS Model Curriculum, and serves as Editor-in-Chief of *Information Systems Management*, Senior Editor of *Data Base*, Associate Editor of *Information Resources Management Journal*, and Editorial Board of *International Journal of Advanced Decision Sciences*. Her research interests include ethical and legal aspects of information technology, system development strategies, and knowledge management.

Burke T. Ward is a Professor in the Department of Marketing and Business Law and is a faculty member of The Graduate Tax Program at Villanova University in Pennsylvania USA. Previously, he was Chair of the Department of Business Law. He was a Visiting Professor at Moscow State Linguistic University in Russia and University of Warsaw in Poland. Dr. Ward earned his LL.M. in Taxation from New York University Law School, and his J.D. from Seton Hall University Law School. He has published numerous articles in the areas of taxation, information systems, and employment law. His current research interests include the legal aspects of information technology, estate planning, and business succession planning.