Information Security as a Business Practice

John Enamait
East Carolina University
jenamait@charter.net

Abstract

This article addresses the role information security plays in an organization. Historically, organizations have deemed information security to be an information technology issue, one that the business as a whole did not need to address. Organizations have also treated information security as an add-on feature, almost an afterthought. Information security must become ingrained into the culture of the organization to ensure security compliance in all facets of the company. Organizations that are beginning to mature with information security may choose to investigate and implement established systems that support information systems. Systems such as ITIL and ISO/IEC 17799 can be used as a foundation for the development of a sound information security process. Regardless of how organizations approach information security, they must begin to envision information security as an overall business problem. If organizations can embrace the cultural change and embrace information security in all aspects of a business, information security will become a well established practice that is followed by all.

1. Introduction

Information security has long been an important component of most organizations. Many organizations have dedicated information technology security departments. While these departments have become more effective at implementing technological it security solutions, information technology security can no longer be isolated to an individual department. Information technology security must become an organizational priority. Even though this is the case, information security has not yet received the necessary attention from many CEOs. Without this top level support, information technology security has often been compartmentalized, with the information technology security department responsible for the organization's information technology security. The individual departments have often been charged with ensuring compliance with federal guidelines such as the Sarbanes-Oxley Act or the Health Insurance Portability and Accountability Act. Unfortunately, legal compliance has been a popular reason businesses have been focusing on information technology security. But implementing security at a departmental level is no longer a viable means to securing an enterprise. In order to combat the increasing threat of Internet crime, organizations must choose to

implement a framework such as ISO/IEC 17799 or ITIL that will allow the organization as a whole to focus on information technology security. Without implementing an organizational framework, businesses will continue to approach security at the departmental level. Unfortunately, this approach has led to avoidable financial losses.

2. Financial Losses

According to *The CGI/FBI Computer Crime and Security Survey* for years 2002 through 2006, the average financial loss due to information security losses have declined. In 2002, a total of 503 organizations reported an average loss of $906,258. In 2003, the number of organizations reporting losses increased to 530. The average loss in 2003 was $380,749. In 2004, an average loss of $286,430 was reported by 494 organizations. The number of respondents was not available for 2005, but the average loss was $204,000. Finally, in 2006, three hundred and eight organizations reported average losses of $167,713. As noted by the declining numbers of organizations reporting financial losses, companies have become reluctant to report computer intrusions to law enforcement authorities. Additionally, these companies have become reluctant to report financial losses due to security breaches. In 2006, only half of the survey participants responded to an anonymous survey seeking this information. This reluctance is derived from the concern of negative publicity an information technology security breach could have on the organization [9]. Even though the information is becoming more difficult to obtain, the data from 2002 – 2006 show that, while the financial losses due to information technology security breaches are significant, the average loss per survey respondent is declining [9]. Even though the average loss is decreasing, companies are still faced with the ever present threat of cyber crime. Robert Richardson, the Computer Security Institute Editorial Director, states "The CSI/FBI survey continues to lend credence to our belief that our survey respondents are getting better and better results from their ongoing focus on information security. But that's not to say that all organizations are protecting themselves with equal vigor. And it's clearer than ever, not only that organizations are always under attack, but that security breaches-especially when widely publicized-can be disastrous both in terms of customer relations and financial results." [9].

The threats these organizations are facing essentially remain the same from year to year. Internet crime is the leading threat to organizations according to forty percent of CIOs and senior level IT managers. Only fifty-nine percent of these believe their IT departments can protect their companies from organized online thieves [1]. According to the Computer Security Institute, virus attacks are responsible for the greatest financial losses. Virus attacks represent 32 percent of the financial losses reported by these organizations [9]. In addition to virus attacks, unauthorized access and theft of proprietary information have increased in severity to organizations. Unauthorized access incidents represented 24 percent of financial losses [9].

3. Security at an Organizational Level

Organizations have historically approached information technology security with a compartmentalized focus. These organizations have been addressing security; however, this focus has been within the scope of an information technology security department within the information technology division. These are organizations that attempt to apply information security at a technological level. The information security department alone has been charged with making the business more secure. While this technical approach is better than doing nothing, Jay Heiser states that there is a problem with approaching information security at a pure technical level. The problem is that most information technology professionals do not understand the business as a whole. Heiser goes on to state that business should "Stop being so technical and allow the business to become totally integrated with security" [6]. Smarter organizations are adopting risk management methods [11]. According to the Global State of Information Security 2004 study conducted by CIO and CSO magazines and PricewaterhouseCoopers, companies are becoming more aware that they must align information security with business objectives [7]. Effective information technology strategies must include a complete understanding of the organizational strategy [5]. However, delegating information security to the information technology department alone can lead to fragmented business and IT plans. Not only can it cause fragmented business and IT plans, but this delegation can cost the business money through mismanaged technology resources [8]. Companies do desire an information security strategy that will address short and long term business needs. In addition to addressing business needs, the strategy must deal with changes in technology [2]. Risk management is being used in the planning and management of information security because risk is a business problem, not a technological one [11]. The alignment of information technology and business processes is a significant issue in most organizations because it directly influences the organizations agility and flexibility to meet business needs [5]. Businesses are beginning to understand the need to take an organizational approach to information technology security. The incentive for this approach may be based more on security compliance rather than on the desire of the chief executive officer.

4. Security Compliance

Information security is a necessity for businesses to remain competitive. Information security also provides for business continuity and legal compliance [4]. Additionally, information security can reduce business interruption [2]. Even though information technology security has distinct benefits for business, not all organizations have implemented consistent levels of information security. In certain business segments, a lack of effective information security can have disastrous consequences. For instance, a hospital lacking effective information technology security processes could inadvertently disclose patient records without the patient's consent. Because of these types of

circumstances, certain compliance requirements have become necessary. A lack of security compliance can have disastrous results for an organization. A business may receive governmental fines, business loss, and civil penalties [4]. Companies often approach information security due to legislation such as the Sarbanes-Oxley Act (SOX) and the Health Insurance Portability and Accountability Act (HIPAA) [4]. A recent survey by Foley & Lardner LLP finds that the number of companies adopting Sarbanes-Oxley (SOX) best practices is growing [3]. Companies are turning to Sarbanes-Oxley for best practice methodologies, among other reasons [3]. According to Claudia Warwar, a managing consultant for IBM's security and privacy practice, "Security today means considering an entire organization and much of its ecosystem of partnerships and relationships – from the network to the workforce, and from the workforce to the supply chain. Meeting this challenge requires an industry-wide approach – no one company can do it alone" [1]. However, only 20 percent of organizations view information security as a CEO-level priority [7].

While information technology security has not become a common CEO priority, due to the nature of implementing security at an organizational level, many companies are hiring chief security officers [4]. The chief security officer is ultimately responsible for knowing which set of legal, business, and financial policies their respective organization must follow [8]. The security officer is then responsible for communicating these requirements to their respective organization [8]. Additionally, the chief security officer is responsible for ensuring that information security becomes an organizational priority. In organizations that have maintained the narrow information technology security focus with individual departments responsible for the organizational security, this task is daunting. In order to move this compartmentalized focus to an organizational one, chief security officers may choose to implement a security framework such as the Information Technology Infrastructure Library or the ISO/IEC 17799.

5. ISO/IEC 17799

Businesses that adopt a security framework must focus on security at an organizational level rather than a technical level. The ISO/IEC 17799 is a framework that offers certification based on the British standard BS 7799. This standard is Britain's information security standard that is used by auditors to certify organizations. The ISO/IEC 17799 framework allows companies to manage information security throughout the enterprise rather than focusing on technical security aspects such as network security in an individual department. Certification is possible using the ISO/IEC framework. By achieving certification, companies are able to publicly state they are able to manage their information security [4]. Also, certification ensures that the entire organization is focused on information security, rather than just focusing on information technology security departmentally.

The ISO/IEC 17799 framework attempts to apply information security aspects at all

levels of an organization including managerial, legal, technical, and operational. The ISO/IEC 17799 framework provides detailed accounts as to how businesses should approach process implementation. Included within the framework are 36 control objectives and 10 security domains. The security domains are:

1. Security Policy – Management commitment and support for information security policy is addressed in this domain.
2. Organizational Security – The coordination and management of the overall organizational information security efforts is detailed in this domain. Also, information security responsibility is defined in this domain.
3. Asset Classification and Control – All critical and/or sensitive assets are defined in this domain.
4. Personnel Security – This domain addresses user awareness and training. User awareness and training can reduce the risk of theft, fraud, and error.
5. Physical and Environmental Security – This domain restricts access to facilities to authorized personnel. Additionally, this domain addresses limiting the amount of damage caused to the physical plant and the organizations information.
6. Communications and Operations Management – This domain addresses the risk of failure and the resulting consequences. This is achieved by ensuring the proper and secure use of information processing facilities.
7. Access Control – This domain ensures the access to respective systems and information is restricted to authorized personnel. The detection of unauthorized activities is also addressed in this domain.
8. Systems Development and Maintenance – This domain addresses the loss and misuse of information in applications used in the enterprise.
9. Business Continuity Management – This domain addresses the ability of the organization to rapidly respond to any interruption of business critical systems. The interruption of these systems may be caused by hardware failures, incidents, and natural disasters.
10. Compliance – This domain addresses legal compliance by the business. Additionally, this domain ensures that the objectives established by top level management are being followed and met.

While ISO-IEC 17799 originated in Europe, many nations have adopted the framework as a national standard. Countries such as Japan, Asia, the Netherlands, New Zealand, and Sweden have all realized the importance of adopting a best practice framework. While other information security frameworks exist, ISO/IEC 17799 is currently the only framework that provides certification. In today's climate of increased legislation, an information security certification could provide an organization

with a documented approach to security compliance.

6. Information Technology Infrastructure Library

The Information Technology Infrastructure Library (ITIL) is another framework companies may choose to adopt. The Information Technology Infrastructure Library originated in Britain in the 1980s. The British government wanted cost-effective and efficient use of its information technology resources. A British governmental agency used the experience of information technology professionals to develop and publish a series of books focusing on best practices. These books became what is now known as ITIL. The guidelines that make up the ITIL framework provide an integrated approach to managing information technology services throughout the enterprise. ITIL is often touted as being able to align information technology with the needs of the business. Not only can ITIL align information technology with the rest of the business, it can also aid in the information security aspects of the business.

Unlike the ISO/IEC 17799 framework, ITIL does not provide detailed accounts as to how a business should approach process implementation. However, ITIL does provide businesses with a framework of what processes should be implemented. ITIL divides activities into processes which have three levels. These three levels are strategic, tactical, and operational. The strategic level is where the organizations objectives are established. The methods to achieving these objectives are also outlined at this level. The second level, the tactical level, is where the specific plan is established for achieving those strategic objectives. Finally, the operational level is where the plan is executed.

The ITIL framework measures integrated information security at each of the three levels. It breaks information security into four distinct categories. These categories include policies, processes, procedures, and work instructions. These four categories help organizations approach information security at the strategic, tactical, and operational levels.

ITIL allows information security to remain focused on the business as a whole. ITIL also serves as the information security foundation. A business may continue to build upon the best practices set forth in the ITIL guidelines. ITIL also prescribes building information security into all IT services throughout the process, rather than after the fact. By building information security throughout the business, this helps prevent a rushed approach to information security to any business service which will save time and money.

The information security process within ITIL includes service level objectives (SLOs) as well as operational level agreements. Service level objectives define the information security requirements in measurable terms. The steps to be taken to achieve the SLO are also included within documentation. Operational level agreements (OLAs) provide descriptions of how information security services will be provided to the business.

ITIL defines three additional information security documents that assist the business. The information security policies provide objectives, goals, and role definitions. The policies are developed by top management and provide direction for the information security efforts of the business. The information security plan illustrates how the policies will be implemented. The plan contains specific information regarding the information system in question or the specific business unit in question. The information security handbook is day-to-day operational guides. Specific working instructions are continued within these handbooks [10].

The information technology strategic plan should consist of seven components [5]:

1. Organizational mission – This component illustrates the overall objectives and strategies of the enterprise.
2. Information inventory – This component provides a summary of information needs for the business. This summary should include both current and future informational needs for the enterprise.
3. Information technology mission and objectives – This component describes the role the information technology department has within the overall organization. Additionally, this component will explain how the information technology department will move the organization from its current state to a position to achieve the organizational objectives.
4. Information technology development constraints – This component describes the limitations faced by the organization in terms of technological and financial resources.
5. Overall systems needs and long-range information technology initiatives – This component provides a summary of the long range initiatives the information technology department has chosen in order to achieve the organizational objectives.
6. Short-term plan – This component provides a summary of current projects and projects to be completed within a year. A certain number of these projects should be taken from the long range initiatives.
7. Conclusions – This component provides a summary of events that may affect the overall plan.

7. Conclusion

ISO/IEC 17799 and ITIL provide businesses with two distinctive approaches to information technology security. These frameworks ensure the organization focuses on information technology security at the enterprise level rather than at a departmental level. Approaching information security at a departmental level has been somewhat effective in the past, but information security now requires an organizational approach. The financial repercussions of ineffective information security can prove disastrous for organizations. The negative

public perception of businesses that are victims of information security breaches has caused many organizations to not report breaches to law enforcement. Additionally, these organizations are hesitant to disclose these breaches and their financial losses to researchers. The lack of companies reporting information regarding information security breaches and their respective financial losses only means the true financial losses are much greater than are reported. Businesses are now faced with a choice regarding information security. They may continue approaching security at the departmental level and apply information security as necessary, or they may adopt a framework that will ingrain security into the organization as a whole. This framework will be the responsibility of the chief security officer, but the chief executive officer is ultimately responsible for the overall performance of the organization. Therefore, the chief executive officer must be the one to lead the business to an implementation of an information security framework such as ISO/IEC 17799 or ITIL.

8. **References**

[1] * Filipek, R. "Online Security Nightmares for CIOs." Internal Auditor 63 (June 2006): 19-20.

[2] * Kolodzinski, Oscar. "Aligning Information Security Imperatives with Business Needs" The CPA Journal 72 (July 2002): 20.

[3] * Nagorski, A. "Sarbanes-Oxley Isn't Just for Public Firms." Internal Auditor 63 (June 2006): 19-20.

[4] * Saint-Germain, Rene. "Information Security Management Best Practice Based on ISO/IEC 17799." The Information Management Journal 39 (July/August 2005): 60-66.

[5] * Shupe, Colleen and Behling, Robert. "Developing and Implementing a Strategy for Technology Deployment." The Information Management Journal 4 (July/August 2006): 52-57.

[6] * Swartz, Nikki. "Gartner: Security is Strategic, Not Technical." The Information Management Journal 39 (November/December 2005): 14.

[7] * Swartz, Nikky. "Businesses Improve Cyber Security." The Information Management Journal 38 (November/December 2004): 18.

[8] Nagaratnam, N., Nadalin, A., Hondo, M., McIntosh, M., and Austel, P. "Business-driven application security: From modeling to managing secure applications." IBM Systems Journal 44 (2005): 847-867.

[9] The Computer Security Institute. "10th CSI/FBI Survey Shows Cybercrime Losses Down For Fourth Straight Year". Retrieved November 22nd, 2006 from http://www.gocsi.com/press/20050714.jhtml

[10] Well, Steven. "How ITIL Can Improve Information Security." (12/22/2004). Retrieved November 14, 2006 from http://www.securityfocus.com/infocus/1815.

[11] Willoughby, Mark. "Security Lessons From Sun Tzu and Hannibal." Computerworld 40 (October 9, 2006): 46.

9. Copyright Notice