A Unified Information Security Management Plan

Mari W. Buche
Michigan Technological University, USA

Chelley Vician
Michigan Technological University, USA

INTRODUCTION

Information is quickly becoming the most significant asset of business practice, and it must be protected and secured in order to be useful. Information security, intrusion detection, and privacy were in the top-10-issues list from the American Institute of Certified Public Accountants (AICPA) survey ("Information Security Heads Top 10," 2003). Furthermore, the potential severity of attacks encourages collaboration between vendors and business clients, including educational institutions, in combating threats (Cox & Kistner, 2003). Essentially, transactions generate data that must be stored for future access in the form of information[1]. Therefore, data integrity is essential because it directly impacts information quality and any decisions based on that information (Brogan & Krupin, 2003; Ross, Stoneburner, Katzke, Johnson, & Swanson, 2003).

To increase confidence in information quality, the information and data must be secured from threats. Information security management must address each of the key areas—confidentiality, authentication, authorization, data integrity, and nonrepudiation—while allowing for continued optimal performance (Gurski, 2003). A rather extreme alternative would be to only distribute needed information to particular individuals, eliminating the necessity of open access to information storage devices (Brogan & Krupin, 2003). However, as the business community strives for integration and sharing of data resources, the criticality of information protection increases, making this an important topic for information systems personnel and systems users (Whitman & Mattord, 2003).

This paper addresses information security management concerns and is divided into five major sections. The first section presents a general discussion of the history of information security management, extending back to the roots of computer security. The next section identifies the key components of information security management, including software, hardware, and human and social elements. This is followed by future trends and concerns relevant to the topic of information security management. Finally, we present our conclusions and general implications for practitioners and academic researchers.

BACKGROUND

Today's discipline of information security has evolved from the early management efforts referred to as computer security (Whitman & Mattord, 2003). Computer security focused on safeguarding physical computing devices and output. Soon after the introduction of computers in office environments, it became apparent that a method for managing the hardware was needed. Locking the office door was usually sufficient for securing the physical computer equipment, as the machines were large and not easily transported. These early computers were initially intended to automate clerical processes, so the actual information generated was not viewed as highly sensitive. Output could be controlled and regulated like all other sensitive artifacts since the output was often in the form of paper printouts.

The lack of integration of the machines contributed to the simplicity of early computer security management (Whitman & Mattord, 2003). Before file sharing became commonplace, files resided in only one location and could be controlled using passwords with relative assurance of protection. Ownership and possession of information could be

easily identified and managed. The advent and ubiquitous nature of the Internet has intensified and complicated the management of information security since no organization controls or manages the vast network of networks (Dhillon, 2003; United States General Accounting Office, 2004; Vijayan, 2003; Weiss, 2004). However, the security of each connected device directly affects the security of every other machine and peripheral on the network. So, management is justified in asserting that security is everyone's business, extending the responsibility beyond security management personnel (Parker, 2003; Verton, 2004).

Legislation is also driving improvements in information security (Johnson, 2004). Two particularly complex regulations pertaining to information technology are the Health Insurance Portability and Accountability Act (HIPAA; Brewin, 2003) and the Sarbanes-Oxley Act in the United States. Both laws make organizations responsible for the protection and control of personal information of patients, customers, and stakeholders. The HIPAA standards have recently been revised to place the burden of risk assessment regarding patient information on the reporting agency. This action decreases the mandated provisions of compliance, but raises the level of accountability for IT managers (Brewin, 2003). The Sarbanes-Oxley Act also places the accountability and responsibility for compliance with the firms' executives. Essentially, business practices need to be reorganized to emphasize privacy and security, embedding security in the processes rather than reacting to breaches in an ad hoc manner (Dhillon, 2003; Gurski, 2003). The legislation is intended to strengthen consumer trust and forge stronger relationships between firms and stakeholders.

INFORMATION SECURITY MANAGEMENT PLAN

Information security involves establishing policies and procedures intended to prevent and/or detect unauthorized intrusions into the organization's information system (Ross et al., 2003; Whitman & Mattord, 2003). Whenever possible, management should combine multiple layers of security to ensure adequate coverage. At the same time, the plan needs to be unified (Johnson, 2004; Myers, 2003; Whitman & Mattord). That is, the separate elements of the information security plan must be managed as a single effort or strategy (Swartz, 2004; U. S. GAO, 2004; Weiss, 2004). As part of the firm's IS strategy, management should perform a risk analysis and determine the appropriate level of security required based on a variety of factors such as possible threats to the network, anticipated damages from expected threats, the probability or likelihood of the threat occurring, and the impact of the information security plan on the organization (e.g., the culture; Whitman & Mattord, 2003). A successful information security management plan must contain policies and procedures that cover multiple dimensions: hardware, software, and people (employees) are the three primary components, as depicted in Figure 1. The major aspects of an information security plan are summarized in Table 1, which provides nine types of barriers to unauthorized access. First, physical security involves the protection of tangible assets by preventing actual access. For example, the computer servers and electronic equipment are secured by preventing physical entry, locking doors, or affixing computers to immovable structures. This is one of the most basic solutions to securing hardware, but is often overlooked in the creation of an information security plan (Berti, 2003). Hackers claim that if they can physically touch a computer, they can hack into the system (Crume, 2000).

Second, personnel controls include the procedures used to limit the access of employees through the use of passwords and security profiles (Jamieson & Handzic, 2003). Passwords must be sufficiently rigorous so that hackers cannot easily break them (Cox & Kistner, 2003; Crume, 2000). To reduce the burden of remembering so many passwords, workers often resort to documenting the codes and placing them near their workstations. Should an unauthorized person gain physical access to the workstation, the list of passwords would allow the individual easy entry into the system. Likewise, security profiles should be established to restrict employee access to only necessary information required in the performance of the job based on the need to know. Exceptions can then be managed on a case-by-case basis, allowing greater access as required to fulfill specific duties.