Information Security Management

Mariana Hentea
Excelsior College, USA

INFORMATION SECURITY MANAGEMENT

Information assurance is a continuous crisis in the digital world. The attackers are winning and efforts to create and maintain a secure environment are proving not very effective. Information assurance is challenged by the application of information security management which is the framework for ensuring the effectiveness of information security controls over information resources. Information security management should "begin with the creation and validation of a security framework, followed by the development of an information security blueprint" (Whitman & Mattord, 2004, p. 210). The framework is the result of the design and validation of a working security plan which is then implemented and maintained using a management model. The framework serves as the basis for the design, selection, and implementation of all subsequent security controls, including information security policies, security education and training programs, and technological controls.

A blueprint can be designed using established security models and practices. The model could be proprietary or based on open standards. The most popular security management model is based on the British Standard 7999 which addresses areas of security management practice. The recent standards, called ISO/IEC 27000 family, include documents such as 27001 IMS Requirements (replaces BS7799:2); 27002, Code of Practice for Information Security Management (new standard number for ISO 17799); and 27006, Guidelines for the accreditation of organizations offering ISMS certification, and several more in development. Similar security models are supported by organizations such as NIST, IETF, and VISA.

From one point of view, information security management evolved on an application of published standards, using various security technologies promoted by the security industry. Quite often, these guidelines conflict with each other or they target only a specific type of organization (e.g., NIST standards are better suited to government organizations). However, building a security control framework focused only on compliance to standards does not allow an organization "to achieve the appropriate security controls to manage risk" (ISM-Community, 2007, p. 27). Besides technical security controls (firewalls, passwords, intrusion detection systems, disaster recovery plans, encryption, virtual private networks, etc.), security of an organization includes other issues that are typically process and people issues such as policies, training, habits, awareness, procedures, and a variety of other less technical and nontechnical issues (Heimerl & Voight, 2005; Tassabehji, 2005). All these factors make security a complex system (Volonino & Robinson, 2004) and a process which is based on interdisciplinary techniques (Maiwald, 2004; Mena, 2004).

While some aspects of information security management changed since the first edition of the chapter (Hentea, 2005), the emerging trends became more prevalent. Therefore, the content of this chapter is organized on providing an update of the security threats and impacts on users and organizations, followed by a discussion on global challenges and standardization impacts, continued with information security management infrastructure needs in another section, followed with a discussion of emerging trends and future research needs for the information security management in the 21st century. The conclusion section is a perspective on the future of the information security management.

SECURITY THREATS ESCALATION AND IMPACT

Reports provided by different organizations include statistics aimed to evaluate the information security field. Although computer security incidents apparently occur with less frequency within organizations, the average losses are up in 2007 compared to previous years (Richardson, 2007). Malware (virus, worms, spyware) losses, which had been the leading cause of loss for the past seven years, fell to second place, after financial fraud and many organizations indicated the presence of

targeted attack (Richardson, 2007). More than 72% of e-mail was spam in May 2007 (Kim, Chung, & Choi, 2007) causing users and providers unnecessary spam-classification expenses.

New types of attacks and malware are fabricated continuously and the degree of sophistication is higher, making the security countermeasures ineffective. Malware is difficult to combat because it spreads quickly or changes the appearance to avoid detection (e.g., poly or metamorphic worms) or perform reconnaissance without infecting vulnerable machines, waiting to pursue strategic spreading plans that can infect thousands of machines within seconds (e.g., flash worms) (Willems, Holz, & Freiling, 2007).

Other types of attacks include phishing, bots, denial of service (DoS), theft of proprietary and confidential information from the mobile device, sabotage of data or networks, laptop or mobile device theft, Web site defacement, and misuse of public Web applications. Statistics (Gaudin, 2007) collected from the first January to the end of May 2007 show an increase of:

- Storm attacks, 10 times larger than any other e-mail attack in the last two years, amassing a botnet of nearly 2 million computers
- Bots, from 2,815 bots in January to almost 2 million bots by the end of July.

Examples of new threats are all or any of the following (Johnson & Goetz, 2007):

- Espionage and organized crime are often difficult to detect and impossible to assess their long-term consequences
- Cyberterrorism
- Contracting, outsourcing, and off-shoring
- Telecommuting, mobile workers
- Social networks
- Insider attacks

Online social networks are emerging constructs that introduce new and potentially severe security risks to business, consumer, government, and academic environments. In addition, more vulnerabilities are discovered within new and old software products:

- Java environment (Vaas, 2007)
- Unicode (Mabry, James, & Ferguson, 2007)
- New operating system Vista and VMware software (Dornan, 2007)
- Potential risk of attacks through pervasive Bluetooth technology with the greatest level of diffusion in smart phones with a rate of 100% per year penetration in the market (Carretoni, Merloni, & Zanero, 2007).

The following section describes global aspects of information security management problems.

GLOBAL CHALLENGES AND STANDARDIZATION

Quite often, dealing with globalization is still challenging because of difficulties for an organization to establish and maintain a strong program within worldwide units (Johnson & Goetz, 2007). The most relevant global challenges include poor software quality and weaknesses of protocols and services. Many vendors for networked devices with a wide range from smart phones to print stations fail to grasp the information security requirement (Oshri, Kotlarsky, & Hirsch, 2007). A large percentage of the security industry is built on the practice of looking for the digital patterns (signatures) that cannot identify unknown threats. One reason is the malware adopting self-mutation to circumvent current detection techniques (Bruschi, Martignoni, & Monga, 2007). Antivirus software based on pattern recognition accounts for more than half of the total security software industry (Richardson, 2007). Also, firewalls employ signature scanning that is flawed and "defenses built on these technologies are increasingly permeable" (Richardson, 2007, p. 3).

New developments as well as sales of the security products are estimated to grow worldwide. Security software revenue will increase at a rate of 10.4% from nearly $8.3 billion in 2006 to more than $13.5 billion in 2011 (Latimer-Livingston & Contu, 2007). The growth is marked also by the continuous demand for improving the security products.

Although IPv6 protocol promises benefits of more secure environment, security threats are already active on IPv6. Network administrators need to be aware that new tools are needed to be used for network troubleshooting and monitoring (Wi-Fi, 2007). As a relatively new standard, security in WiMAX (Worlwide Interoperability for Microwave Access) networks has only been addressed in a few studies (Lu, Qian, & Chen, 2007). Also, increased developments based on