Road Map to Information Security Management

Lech Janczewski
The University of Auckland, New Zealand

THE INFORMATION SECURITY ISSUES

Developments in multimedia technology and in networking offer to organizations new and more effective ways of conducting their businesses. That includes both internal as well as external contacts. Practically every business person owns a mobile phone, has PDA/laptop with wireless capabilities, and is able to communicate with colleagues/clients all over the world and from every place on the globe. As a result, well defined barriers between different organizations are becoming less and less visible. This technical progress intensifies the competing forces. In the past, an organization was directly exposed to competition located within their city or region. Now, due to easy communication, their competitor could be located on the opposite side of the globe.

The advantage of using multimedia technology and networking could be accomplished only if data handled by a company are *secure*, that is, are available only to the authorised persons (*confidentiality*), represent true values (i.e., had not been changed during storage, processing, or transport), and are available on demand (*availability*). Thus, managing security of information becomes an obligatory part of running any modern IT system. There is not absolute IT system security. If a system is accessible by authorised people, by definition it is impossible to eliminate chances of unauthorised access. However, proper means exist to dramatically decrease the probability of occurrence of such unauthorised activities.

This article illustrates the importance of proper managing in information security processes in an organization and presents a first level guidance on how to approach this problem. The most widely known document on information security is an annual *Computer Crime and Security Survey (CCSS)*, conducted by San Francisco's Computer Security Institute in cooperation with the FBI (CSI, 2006). It is based on responses from over 500 professionals representing all types and sizes of organizations from huge international corporations to small businesses from nationwide government agencies to small community centres. The message the survey is conveying is frightening:

- Total losses for 2006 were $52,494,290 (USD) for the 313 respondents that were willing and able to estimate losses.
- Losses due to virus contamination caused the most significant loss (over $15 million).
- Unauthorised access to information was the second-most expensive computer crime among survey respondents.
- As in previous years, virus incidents (65.2%) and insider abuse of network access (47%) were the most cited forms of attack or abuse.
- The impact of the Sarbanes–Oxley Act on information security continues to be substantial. In fact, in open-ended comments, respondents noted that regulatory compliance related to information security is among the most critical security issues they face.

The report is covering only a very small part of the USA's economy, and real nationwide losses could be several magnitudes higher. Surveys of a similar nature are conducted in many other countries like New Zealand (NZ Survey, 2005; AusCERT, 2003). These surveys brought similar results. It is not a surprise, as the whole globe is becoming a wired village and the computer technology is the same all over the world.

These alarming facts are now a major worry of the business community. This is reflected in surveys asking organization executives what their main points of concern are and which activities they consider the most important. Two decades ago, the information security issues were nonexistent in these surveys. They had appeared on the top-ten list around the early 1990s, and they are gradually progressing toward the top. Bombarded by the flood of warnings about possible damages from the misuses of information technology, the managers switched to investing in security

measures. However, these investments are done quite reluctantly. The nature of threats is still mysterious to nonspecialists, and one of the most common statements is: "Why should I invest in information security when we did not register any abuses or attacks?"

Unfortunately, unlike bank robbery, many attacks against computers may go unnoticed. They are difficult to notice and thus impossible to launch an investigation around. The classical example is hacking—attempts to gain unauthorised access to computer resources. If the hacker was either unable to break into the system or did not change any records, then such an attempt would remain unknown if the installation did not have any hacker-detecting tools. The other point is that the effects of computer frauds are difficult to notice: an successful attack removing $30,000 from accounts of a company processing weekly millions of dollars may go unnoticed for a long period of time allowing the perpetrators to cover their steps. The possible consequences could emerge much later and may not necessarily point to a particular hacker attack.

Of course, ordinary information systems with highly sensitive information need protection from hackers. Intrusion detection methods have been developing over the past half-decade largely in response to corporate and government break-ins (Durst, Champion, Witten, Miller, & Spagnuolo, 1999). In many cases, when appropriate detection tools had been installed, the information technology managers were terrified to learn about the extent of their system abuses.

There are two essential strategies for protection of network infrastructures. One strategy is a "terminal defence" initiative undertaken by the owners of individual nodes in a network to protect their individual nodes from persistent, well-supported intrusion. The other strategy is a "collective action" that involves groups of owners, industry groups, government groups, and so forth, who audit the collective system operation and exchange information to detect patterns of distributed attacks. Collective action can also involve redundant capacity across the collective system and the ability to reallocate a system load or to ration diminished system capacity. Both strategies can also involve preventative measures, such as research and development to improve the state of the art in system security or the exchange of threat and countermeasure information (Lukasik, Greenberg, & Goodman, 1998).

Intrusion detection attempts to discover attacks, preferably discover them while they are in progress, or at least discover them before much damage has been done. Automation of intrusion detection is typically premised on automated definition of misuse instances. This automation requires pattern recognition techniques across large databases of historical data. Methods for data mining clearly have contributed to making such intrusion detection feasible (Bass, 2000; Zhu, Premkumar, Zhang, & Chu, 2001). These approaches have been growing in sophistication and include expert systems, keystroke monitoring, state transition analysis, pattern matching, and protocol analysis (Biermann, Cloete, & Venter, 2001; Graham, 2001). However, intrusion detection approaches thus far remain a probabilistic enterprise with less than a 100% chance of detecting all types of intrusion. Indeed, the race between intruder technology and intrusion detection will likely remain a closely run contest. A new tool makes attacks undetectable. Intrusion detection tools are necessary but not sufficient for the high-stakes information resources subject to attacks.

The predominant approach to information security is often labeled *piecemeal approach*. Many information security tools are well known like firewalls or virus scanners. Under the piecemeal approach, the user sees the danger of a specific threat, identifies tool(s) to reduce such a threat, and implements this tool. Such an approach may work but would not necessarily render the optimal solution from the overall perspective of business organization.

INFORMATION SECURITY MANAGEMENT

A *system approach* is a top-down methodology of developing an information security system recommended in the literature. It is based on an IBM-developed methodology of investing in information technology called business system planning (BSP) (Zachman, 1982). The process presented next is a modification of that methodology to the needs of information security. The ten basic steps of the methodology are presented in Figure 1.

Step 1: Managerial Drive

The building of a sound security system should be initiated, endorsed, supported, and controlled by top management. The IT personnel may have a very sound