Road Map to Information Security Management

Lech J. Janczewski
The University of Auckland, New Zealand

Victor Portougal
The University of Auckland, New Zealand

INFORMATION SECURITY ISSUES

Developments in multimedia technology and networking offer organizations new and more effective ways of conducting their businesses. That includes intensification of external contacts. Barriers between different organizations are becoming less visible. The progress gives advantages to competing forces, as well. In the past, an organization was directly exposed to competition only within its own region. Now, due to easy communications, a competitor could be located on the opposite side of the globe, having the ability to access or even disrupt the most sensitive information of a competing company. Hackers and other cyber-criminals are another part of the external threat.

Thus, advantages of using multimedia technology and networking could be accomplished only if data handled by a company are *secure* – available only to the authorised persons (*confidentiality*); represent true values – are not changed during storage, processing or transport (*integrity*); and are available on demand (*availability*). Managing security of information becomes an essential part of running any modern IT system.

This article presents a first-level guidance for 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 Federal Bureau of Investigation (FBI) (CSI, 2003). It is based on responses from more than 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 conveys is frightening:

- The total annual losses reported in the 2003 survey were more than $200 million.
- As in prior years, theft of proprietary information caused the greatest financial loss (more than $70 million was lost, with the average reported loss being approximately $2.7 million).
- In a shift from previous years, the second most expensive computer crime among survey respondents was denial of service, with a cost of $65 million.
- Losses reported for financial fraud were significantly lower, at $10 million.
- As in previous years, virus incidents (82%) and insider abuse of network access (80%) were the most cited forms of attack or abuse.

The report is covering only a very small part of the United States' (U.S.) economy; real nationwide losses could be several magnitudes higher. Surveys of a similar nature are conducted in many other countries, like Australia (AusCERT, 2003). These surveys brought similar results. It is not a surprise, as the whole globe is becoming a wired village, and 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, information security issues were nonexistent in these surveys. They had appeared on the "Top 10" list around the early 1990s, and they are gradually making their way towards the top. Bombarded by the flood of warnings about possible damages from the misuses of information technology, managers switched to investing in security measures. However, these investments are done quite reluctantly. The nature of

threats is still mysterious to non-specialists, 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 are difficult to notice and thus impossible on which to launch an investigation. 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 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.

Two essential strategies exist for protection of network infrastructures. One 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 preventive 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 while they are in progress or at least 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).

But intrusion detection approaches thus far remain a probabilistic enterprise, with less than 100% chance of detecting all types of intrusion. Indeed, the race between intruder technology and intrusion detection will likely remain a closely run contest. New tools make attacks undetectable. Intrusion detection tools are necessary, but not sufficient for the high-stakes information resources subject to attacks.

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

INFORMATION SECURITY MANAGEMENT

System approach is a top-down methodology of developing an information security system recommended in literature. It is based on an IBM-developed methodology of investing in information technology called Business System Planning. The following process is a modification of that methodology to the needs of information security. The basic 10 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 the top management. The IT personnel may have a very sound understanding of the information security processes or of their importance, but without top management's understanding and active support, introduction of an effective security system is impossible.