# Chapter 7
## Securing Information Systems

**LEARNING TRACK 2: MANAGEMENT CHALLENGES OF SECURITY AND CONTROL**

Information systems security needs organizational and management resources as well as technologies. Establishing a good framework for security and control requires skillful balancing of risks, rewards, and the firm's operational capabilities.

## Opportunities

Information system security and control are more crucial than ever. Firms today have opportunities to create marvellously secure, reliable Web sites and systems that can support their e-commerce and e-business strategies. On the downside, revenue, liability, reputation, brand image—and even a company's ability to survive—will suffer if a firm is found to be insecure or unreliable. The stakes have never been higher.

## Management Challenges

There are many alternative technologies to help firms achieve security and control, but organizational discipline is required to use these technologies effectively.

### DESIGNING SYSTEMS THAT ARE NEITHER OVERCONTROLLED NOR UNDERCONTROLLED

Although security breaches and damage to information systems still come from organizational insiders, security breaches from outside the organization are increasing because firms pursuing electronic commerce are open to outsiders through the Internet. It is difficult for organizations to determine how open or closed their networks should be to protect themselves. If a system requires too many passwords, authorizations, or levels of security to access information, the system will go unused and therefore is ineffective. Controls that are effective but that do not discourage authorized individuals from using a system are difficult to design.

### IMPLEMENTING AN EFFECTIVE SECURITY POLICY

Despite increased awareness of worms, denial of service attacks, and computer crime, far too many firms do not pay sufficient attention to security. Controls and security programs are often treated as an afterthought rather than incorporated into the design of key business processes and systems. Research has shown that 75 percent of companies with information security policies do not keep them up-to-date and that only 9 percent of employees understand these security policies. Many firms lack disaster recovery and business continuity plans or fail to patch their software routinely against security vulnerabilities. Managers do not appreciate the value of a sound security strategy. Security threats abound, but they are neither predictable nor finite, making it more difficult to calculate returns on security investments. Unless managers change their thinking about security, security budgets will be inadequate.

## Solution Guidelines

One thing is clear: Security and control must become a more visible and explicit priority and area of information systems investment, with greater emphasis on the overall organizational planning process. Coordinating the firm's security plan with its overall business plan shows that security is just as essential to the success of the business as any other business function. Larger firms may merit a formal security function with a chief security officer (CSO). To develop sound security and controls, users may need to change the way they work. Support and commitment from top management is required to show that security is indeed a corporate priority and vital to all aspects of the business.

Security and control will never be a high priority unless there is security awareness throughout the firm. Security and control should be the responsibility of everyone in the organization. Users may need special training on how to protect equipment and passwords and how to work with antivirus and other protective software. Key management decisions include determining an appropriate level of control for the organization and establishing standards for system accuracy and reliability. Managers should ask the following questions:

- What firm resources are the most critical to control and secure? How much would it cost to replace these critical assets if they were destroyed or compromised? What would be the legal and business impact if they were accessed by unauthorized parties?
- What level of system downtime is acceptable? How much disruption in business function or financial loss is the business willing to tolerate?
- What is the minimum acceptable level of performance for software and systems? If zero defects are impossible to achieve in large complex pieces of software, what constitutes acceptable, if not perfect, software performance?
- How much is the business willing to invest to protect its information assets?