

Executive Management of Information Security

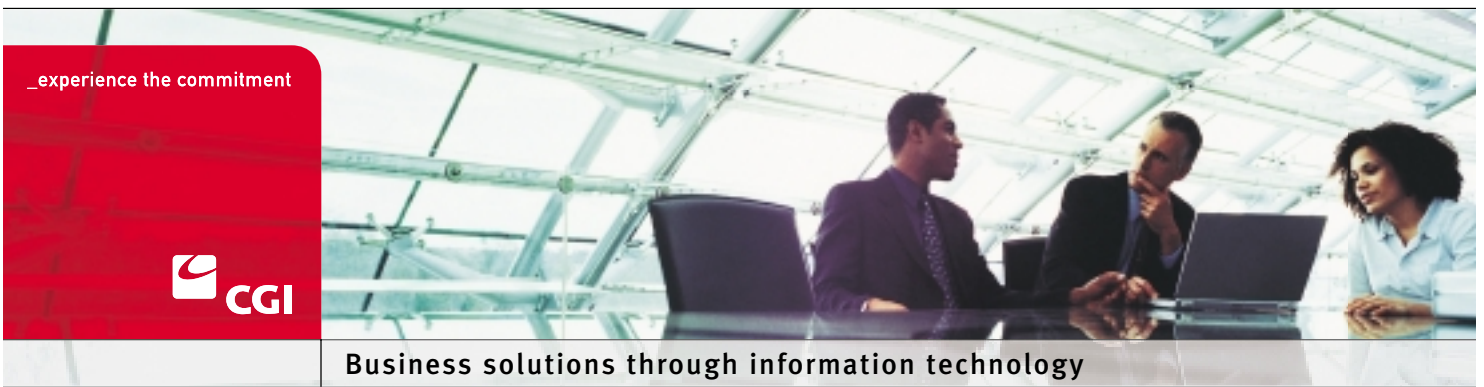


TABLE OF CONTENTS

WHY SECURITY DEMANDS EXECUTIVE-LEVEL ATTENTION	3
DEFINE NOTES AND RESPONSIBILITIES	4
DEVELOP POLICIES AND PROCEDURES	4
PROMOTE AWARENESS AND FACILITATE COORDINATION	4
MONITOR AND TRAIN	5
CONCLUSION	5
ABOUT CGI	5

Why security demands executive-level attention

In today's technology-driven business world, it has become critically important for companies to safeguard their information assets, systems and networks. While the technology revolution has generated vast benefits, it has also exposed companies to new risks and liabilities. The shift from centralized to distributed computing environments has made valuable information and IT assets more vulnerable to internal and external attacks. A proliferation of computer literates and readily available hacking tools has also raised the odds of attack. Viruses, Web site defacements, privacy violations, theft and other security breaches have become increasingly commonplace, resulting in financial losses, legal liability, damaged reputations and decreased shareholder confidence.

In fact, recent years have seen an unprecedented rise in cyber crime and related malicious activity. Results of the 2003 Computer Crime and Security Survey conducted by the Computer Security Institute and the FBI show the threat continues unabated. Ninety-two percent of the survey's 530 respondents reported attacks during the past year and, of the 251 organizations that were able to quantify their losses, total damages exceeded \$200 million.

The risk and potential damage of information security breaches have led to new and emerging laws and regulations at the national and international level holding corporations and their executives liable for security and privacy violations. Legal experts also predict a surge in tort liability lawsuits filed by injured parties against companies for having inadequate security.

For these reasons, information security is moving up on the list of corporate priorities. Viewed no longer as just an IT issue, it is increasingly drawing the attention of senior management as a mission-critical initiative. More and more companies are turning to outside experts to help secure their organizations, leading to rapid growth in the security services market. In North America, alone, Gartner predicts the market is expected to grow from \$4.1 billion in 2001 to nearly \$9 billion in 2006.

Steps executives should take to ensure security

The intense focus on security is leading corporate boards to mandate the establishment of information security infrastructures within their organizations. Boards are calling on executive management, not IT departments, to recommend, develop and implement these infrastructures to protect the company from security breaches and legal liability. For many executives, this is a new discipline and the lack of proper direction spell outs potential disaster.

Define roles and responsibilities

The key to success with any type of infrastructure management program is focus. Establishing and maintaining an effective security infrastructure is no exception. A major challenge in most cases is deciding who should be responsible for handling security. Ideally, overall responsibility should be assigned to a Chief Security Officer (CSO). At a minimum, the CSO role should be combined with that of either the Chief Technology Officer (CTO) or Chief Information Officer (CIO).

Combining roles is advisable only in a situation where one person can reasonably manage the combined responsibilities and there is no potential conflict of interest. The CSO's primary responsibility to the board is effective risk management and mitigation. Combining the CSO role with another could potentially result in a conflict of interest jeopardizing the fulfillment of this responsibility. In cases where the CSO role is combined with another, appropriate controls must be carefully put in place and monitored to ensure a conflict does not arise.

Hiring trained and experienced information security professionals is also fundamental to

success. Securing an entire organization is a complex and dynamic process, requiring significant expertise. There are a number of internationally recognized professional certifications available to demonstrate an individual's proficiency in information security. Some of the most prominent certification organizations are listed below.

Certification Organizations		
Organization	Certification	Comments
ISC ²	CISSP	http://www.isc2.org
ISACA	CISA CISM	http://www.isaca.org
SANS	GIAC	http://www.sans.org , http://www.giac.org
ISSA	N/A	http://www.issa.org/certification.html
DRI	CBCP MBCP	http://www.dri.ca

Develop policies and procedures

Only after roles and responsibilities have been clearly defined can one begin to tackle the challenge of actually establishing and managing an information security infrastructure. To achieve maximum effectiveness, the concept of information security as a continually expanding and evolving discipline must be thoroughly understood and embedded within the organization. Further, all components of the information security infrastructure must be fully integrated with each other and with the daily operations of the business.

The key to integration lies within the organization's policies and procedures. Policies and procedures send a clear message throughout the organization that executive management is committed to a set of standards along with methodologies for implementing those standards. Coupled with a clearly defined flow of responsibility, policies and procedures provide a strong foundation upon which security measures can be put in place and enforced.

One of the best resources to guide executives in developing policies and procedures is the International Organization for Standardization (ISO). ISO has developed ISO 17799—a comprehensive set of best practices for information security management. Adopted from its predecessor, the British Standard 7799, ISO 17799 is the most widely recognized security standard in the world today. It divides the overall information security function into several levels and recommends areas where policies and procedures are essential. More information about ISO 17799 and BS 7799 is available at <http://www.iso.org> or <http://www.bsi-global.com>.

Promote awareness and facilitate coordination

Once policies and procedures have been documented and accepted by the board and senior management, awareness must be generated throughout the organization. Users need to understand how the policies and procedures impact them, as well as management's compliance expectations.

An important responsibility of the CSO is to liaison with different departments within the organization to promote awareness of security at the departmental level and coordinate the

enforcement of security practices. Key departments involved in this coordination effort include human resources, facilities management, IT and auditing. These departments depend heavily on the CSO to ensure they are working effectively with each other in handling security-related issues and concerns.

The CSO must also closely align information security measures with corporate directives, including business continuity and disaster recovery, as part of his risk mitigation role. As such, the CSO is typically involved in managing and coordinating organizational business continuity and disaster recovery plans.

Monitor and train

Strong security management also involves continual monitoring and security awareness training. Errors and omissions are still one of the leading causes of security breaches. Monitoring ensures ongoing compliance with policies, procedures and legislation. It also fosters accountability and facilitates auditing. In addition, monitoring provides the basis for enforcing policies and procedures by identifying where, when, how and by whom security breaches occur.

Security awareness training serves two primary purposes if conducted on a regular basis. First, it delivers critical information to those in the organization who need it most—the general workforce. Second, it serves as a continual reminder that security is a key aspect of day-to-day operations.

While the CSO should be responsible for overseeing monitoring and enforcement efforts, actually performing these duties could result in a conflict of interest. The same applies to IT staff. IT staff may be assigned the responsibility of procuring monitoring and enforcement tools. However, they should not be charged with reviewing logged data based on the principle of separating duties as a means of control.

Conclusion

Information security management is a vast undertaking, crossing all divisions and departments within an organization. No technology-dependent organization is exempt from the need to implement effective security measures as part of an enterprise-wide management program. The responsibility for directing the development of security initiatives rests with executive management. Minimizing security breaches and avoiding legal liability depends on executive management taking the necessary steps to develop an effective information security infrastructure. Executives should take the time to understand their organization's security issues and drive the development of policies and procedures to ensure the highest level of security possible and their organization's future success.

About CGI

Founded 1976, CGI has worked with clients in a wide range of industries to help them leverage the strengths of information technology (IT) to optimize their business performance and produce value-driven results. We also offer a comprehensive array of business process outsourcing (BPO) services, enabling us to help manage and improve our clients' day-to-day business processes while freeing them up to focus more on strategic decision making. Our consulting, systems integration and outsourcing services provide a total solution package designed to meet our clients' complete business and technology needs. We approach every engagement with one objective in mind—to help our client win and grow. CGI provides services to clients worldwide from offices in Canada, the United States, Europe, as well as centers of excellence in India and Canada.

To explore this topic and how we can help, contact your CGI account manager or visit http://www.cgi.com/web/en/head_office.htm for the location of the CGI office nearest you. Other information about CGI can be found at www.cgi.com.