



WHITE PAPER

Executive Management of Information Security



_experience the commitment™

TABLE OF CONTENTS

WHY SECURITY DEMANDS EXECUTIVE-LEVEL ATTENTION	3
STEPS EXECUTIVES SHOULD TAKE TO ENSURE SECURITY	4
- DEFINE ROLES AND RESPONSIBILITIES	4
- DEVELOP POLICIES AND PROCEDURES	5
- PROMOTE AWARENESS AND FACILITATE COORDINATION	5
- MONITOR AND TRAIN	6
CONCLUSION	6
ABOUT CGI	6

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 2009 Computer Crime and Security Survey conducted by the Computer Security Institute (gocsi.com) highlights that threats continue to evolve unabated. Of the survey's 443 respondents, one-third of respondents' organizations were fraudulently represented as the sender of a phishing message and reported big jumps in incidence of password sniffing, financial fraud and malware infection. When asked what security solutions ranked highest on their wish lists, many respondents named tools that would improve their visibility—better log management, security information and event management, security data visualization, security dashboards and the like.

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. Several of these regulations have very strict and auditable requirements that companies are required to meet such as the Sarbanes-Oxley Act (SOX), Payment Card Industry (PCI DSS) and health information privacy (HIPAA in USA / PIPEDA in Canada). Legal experts also predict a surge in 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. Security is getting a larger slice of the IT budget pie," says Forrester analyst Jonathan Penn in a 2009 enterprise study. "Firms are devoting 11.7 percent of their company's IT operating budget to IT security in 2008—contrasted with 7.2 percent in 2007—and plan to continue nudging up IT security budgets in 2009 to 12.6 percent of the IT operating budget." Security will also account for a higher percentage of budget allocations for new initiatives this year, going from 17.7 percent in 2008 to 18.5 percent in 2009, the report says.

Similar increases are expected in smaller companies, Penn says in the SMB report. “SMBs devoted 9.1 percent of their companies’ IT operating budget to IT security in 2008—down from 9.4 percent in 2007—but they have plans to bring IT security budgets back up to 10.1 percent in 2009,” the report says. “Allocation of budget for new initiatives mirrors this trend, with security going from 14.9 percent in 2008 to 15.9 percent in 2009. No big swings of the budget axe here.”

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
DRI	GIAC	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 ISO/IEC Information Centre jointly operated by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). Together they have developed ISO/IEC 27000 series—a comprehensive set of best practices for information security management. Adopted from its predecessors, the British Standard 7799 and ISO 17799, the 27000 series 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/IEC 27000:2009 (overview document) and key standards ISO/IEC 27001:2005 (Security Management System requirements) and ISO/IEC 27002:2005 (IT Security best practices and controls) is available at <http://www.iso.org>.

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

At CGI, we're in the business of satisfying clients by helping them win and grow. For more than 30 years, we've operated upon the principles of sharing in clients' challenges and delivering quality services to address them.

As a leading IT and business process services provider, CGI has a strong base of 26,000 professionals operating in more than 100 offices worldwide, giving us the competitive advantage of close proximity to our clients. Through these offices, we offer local partnerships and a balanced blend of global delivery options to ensure clients receive the optimal combination of value and expertise required for their success.

We define success by helping our clients achieve superior performance and gain competitive advantage.