

Information security in enterprise management: Making security an integral part of an organization's overall IT and business strategy

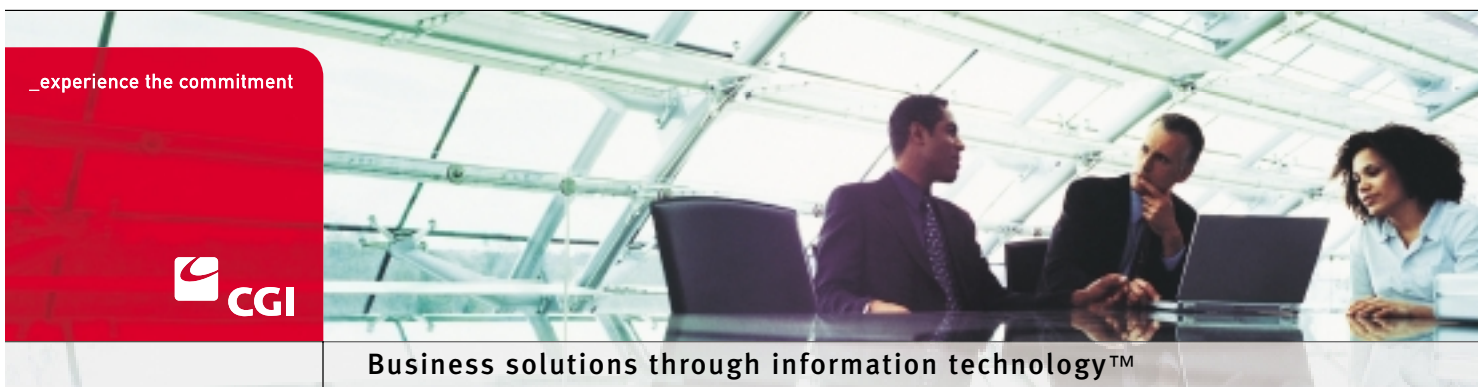


TABLE OF CONTENTS

INTRODUCTION	3
THE THREAT	3
CYBER THREATS EMERGE	3
NO BORDERS	4
A HIDDEN PROBLEM	4
TACKLING THE PROBLEM	5
THE PERIMETER FOCUS	5
A BROADER APPROACH	5
LARGER CORPORATE DEMANDS	5
PRIVACY STANDARDS EMERGE	6
THE RISE OF GOVERNANCE	6
INTO THE BOARDROOM	6
SECURITY WITHIN ENTERPRISE MANAGEMENT	7
A BUSINESS ENABLER	7
EMERGING BUSINESS-FOCUSED FRAMEWORKS	7
ELEMENTS OF EFFECTIVE SECURITY MANAGEMENT	9
LOOKING FORWARD	12
SECURITY AS PART OF THE EXECUTIVE TEAM	12
ENTERPRISE-WIDE SECURITY INTEGRATION	12
PARTNERING FOR STRENGTH	12
CONCLUSIONS	13
ABOUT CGI	14

Rapid advances in technology have brought new opportunities for organizations to extend their reach and enhance their services. Yet with all the advantages of the information age, organizations are also experiencing new vulnerabilities. As rates of security incidents continue to rise, organizations are shifting from viewing information security as a defensive strategy to an integral part of their organization's overall IT and business posture. Enterprise security management encompasses the governance, strategies, frameworks, plans and assessments necessary to create and manage an effective enterprise-wide security program.

Introduction

Perhaps more than any other time in history, recent political and business events have shaped security perceptions and generated strategic security initiatives. A recent survey¹ of more than 800 respondents, for example, estimates that computer-based criminal activity in the United States results in an annual loss of more than US\$150 million—and this does not include loss of productivity and potential earnings due to virus attacks, denial of service, SPAM, information loss and so on. As demonstrated by this survey and others, an alarming increase in security risks threaten activities that rely on customer confidence, such as online banking and electronic access to government services, making the success of these activities dependent on effective measures to protect the security of transactions, information and resources.

Today's security threats raise many questions for organizations: How do we address security? How does it fit with concurrent demands for good governance, regulatory compliance, best practices and management frameworks? How do we instill confidence and maintain equilibrium between threats, risks, integrity and trust?

This paper examines these and other issues related to the development of a comprehensive and integrated approach to security. Primarily intended for senior managers and enterprise planners in commercial and government organizations, it provides an overview of emerging threats, as well as common perceptions and responses to those threats. It also briefly describes how information security has matured to become an element of business management—an essential step toward the preservation of corporate integrity and assets. To this end, the paper concludes with a number of recommendations on how to develop an effective security management strategy.

The threat

Cyber threats emerge

Security has long been a consideration for those responsible for computing systems. Over the years, the level of threat and the need for corresponding safeguards have varied, depending on the environment in which the systems were deployed and the data they processed. However, with the proliferation of computers, electronic information and exploding public access to online technology, a new dimension in security became increasingly apparent—the Internet.

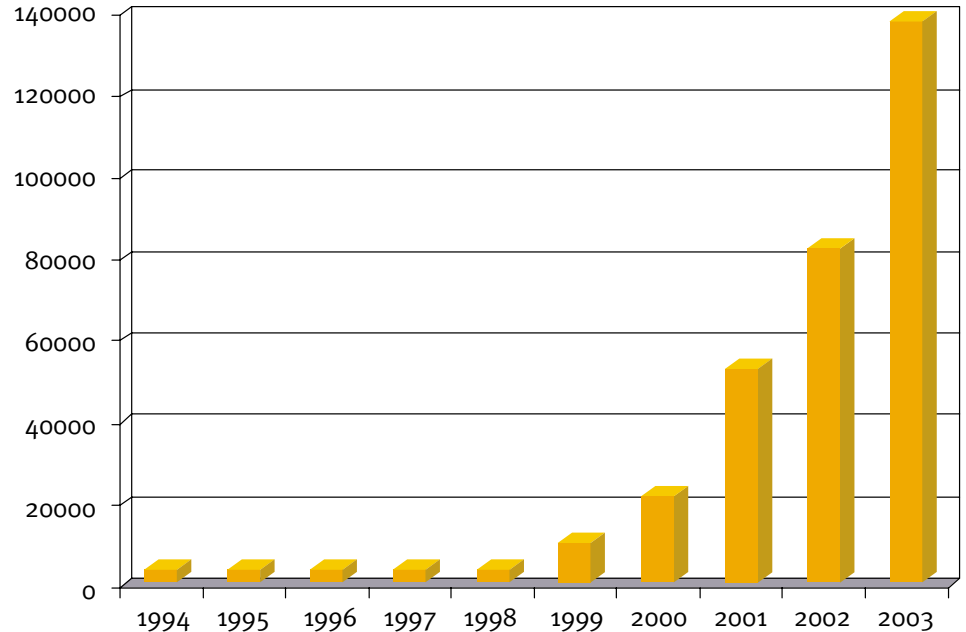
The Internet marked the beginning of a new social and commercial phenomenon. It also opened a door for those seeking to electronically exploit others' data and infrastructure for their own purposes. Often collectively referred to by the misnomer "hackers," this group included fraud artists, thrill seekers, cyber-vandals, saboteurs and scammers, as well as those conducting corporate, industrial and government espionage. At risk were government and corporate networks that operated as private air-gapped networks, but were now becoming increasingly connected to the outside world.

By convention, threat trends have usually been defined in terms of the number of security "incidents." The Computer Emergency Response Center, an authoritative information security body operated by Carnegie Mellon University's Software Engineering Institute, defines an "incident" as "the act of violating an explicit or implied security policy." This includes, but is not limited to, the following:

- Attempts, either failed or successful, to gain unauthorized access to a system or its data
- Unwanted disruption or denial of service
- Unauthorized use of a system for processing or storing data
- Changes to system hardware, firmware or software characteristics without the owner's knowledge, instruction or consent

Based upon this definition, the graph below clearly demonstrates an exponential rise in the number of security incidents during the period 1994–2003.

Reported security incidents 1994–2003



Data Source: Carnegie Mellon Software Engineering Institute CERT Coordination Center

No borders

The fact that access to electronic information has no geographic boundaries became clear in early 1998, when a series of attacks were launched over the Internet against web and email servers at the Massachusetts Institute of Technology (MIT) Plasma Science and Fusion Center, as well as a variety of government sites including those belonging to NASA and the Pentagon. The initial perpetrators were stereotypical hackers—high school students in Northern California. However, their mentor and the perpetrator of follow-on attacks was a 20-year-old Israeli hacker who led a ring of apprentices responsible for routinely attacking government and military systems, and possessing the tools necessary to attack credit card systems.

Similar attacks against North American targets were also launched from Europe during the same time period. Highly publicized at the time, these attacks demonstrated that borders were irrelevant with respect to information security. They also served to create a broader public awareness of the need for computer security and raised the bar on threat perceptions.

A hidden problem

For years, the true scope of the security problem remained largely hidden, especially in large, publicly traded companies in industries such as banking and finance. Although corporations experienced attacks against their IT infrastructures, they often refused to acknowledge them for fear that doing so would inspire more attacks, undermine confidence in the integrity of their infrastructures, and raise questions about their ability to protect assets. Commenting on the results of the 2004 E-Crime Watch Survey data, Larry Johnson, special agent in charge of the Criminal Investigation Division of the U.S. Secret Service stated, "Many companies are still unwilling to report e-crime for fear of damaging their reputation. However, as we see with this survey, ignoring the problem or dealing with it quietly is not working."² Similarly, government agencies were experiencing attacks, but many were not reported for security reasons.

Meanwhile, on a broader scale, issues such as the much-publicized Y2K software "vulnerabilities" demonstrated to the private and public sectors exactly how extensive and complex their infrastructure and system dependencies were—and just how fragile they could be. They began to realize that just hiding or ignoring the problem would not make it go away.

Tackling the problem

The perimeter focus

Highly visible "hacker" events served to focus industry attention on the external threat. To a great extent, preoccupation with creating a "hard perimeter" persists to date, despite the fact that analyst firms such as Gartner Group have long maintained that between 60 and 75 percent of all IT security incidents occur from within—inside the armored boundary that many organizations have created.³

Although the numbers are decreasing as broader security strategies are adopted, many senior security officers still admit they maintain a posture that is primarily directed at outside threats. According to the 2004 E-Crime Watch survey⁴, more than half (52 percent) of corporate information security officers (CISOs) say they have a "moat and castle" approach to network security, admitting that once the perimeter is penetrated, the inner defenses are soft. It is clear that both internal and external threats must be addressed within a comprehensive security strategy that includes vigilance, defense in depth and internal risk containment/damage limitation.

A broader approach

Over the past 10 years, security has undergone a slow process of change and maturation that continues to date. How private industry and government viewed the scope and depth of security began to change as management realized that the key pillars of security—confidentiality, integrity and assurance—meant more than just stopping hackers at a firewall. They began to realize that these pillars are fundamental to the establishment of trust. Thus, long before 9/11, many Western countries began to look at national infrastructure protection policies that took a much broader approach toward information technology and security issues within the larger, more strategic context of protecting vital assets and sustaining core capabilities and business functions.

In Canada, the larger strategic context of security and the protection of business functions were brought into further focus by a 1998 ice storm in the eastern sections of Canada and the United States, which caused widespread power outages and business disruption. These and other events contributed to the formation of the Office of Critical Infrastructure Protection (OC�PEP) in Canada in February 2001, some seven months before the 9/11 attacks, which forever changed how the world regarded security in general.

Larger corporate demands

Although securing enterprise assets and infrastructure was seen as an area of growing importance, it was certainly not the principal focus for corporate management. Instead, security emerged as a key supporting component of good governance, corporate responsibility, transparency and accountability. By the early 1990s, the industry had already developed several IT management best practice frameworks, such as CobiT (Control Objects for Information and related Technology) and ITIL (Information Technology Infrastructure Library). In the UK, ISO (International Organization for Standards) 17799 was first established as the DTI code of practice and later rebadged as version 1 of BS7799 in February 1995. This set of security-related standards was subsequently published as the ISO 17799 standards in December 2000 and was updated as version ISO/IEC 17799:2005 in June 2005.

"Fundamentally, [governance] is about power, relationships and accountability: who has influence, who decides, and how decision-makers are held accountable. While good governance can be seen as an end unto itself, it is also a process that can be undertaken by any number of actors, and is not solely tied to the institutions of government."

— Tim Plumptre, president of Canadian think-tank Institute on Governance (<http://www.iog.ca>)

Privacy standards emerge

Meanwhile, in 1996 the U.S. Congress enacted the Health Insurance Portability and Accountability Act (HIPAA), requiring the creation of standards intended to protect the privacy of individually identifiable health information. A corresponding set of privacy standards with important security implications were put in place in December 2000. In Canada, comprehensive privacy legislation was instituted in the form of the Personal Information Protection and Electronic Documents Act (PIPEDA) in April 2000. Although less far-reaching, a number of individual privacy regulations and directives were also implemented in the UK during the same period.

The rise of governance

More recently, Enron, Worldcom and other private-sector scandals, as well as contracting and procurement scandals in government, have resulted in the implementation of a series of broad policy and legislative measures aimed at ensuring that corporate boardrooms exercise their responsibilities by maintaining sound business practices. Included among these changes are policies and measures aimed at ensuring the security and integrity of the enterprise and its assets. Examples include:

- Sarbanes-Oxley Act of 2002
- Treasury Board of Canada Secretariat Management Accountability Framework
- Treasury Board of Canada Integrated Risk Management Framework
- Government of Canada, Operational Security Standard: Management of Information Technology Security (MITS)
- Updates to the Government of Canada, Government Security Policy: Operational Standard for the Security of Information Act, March 17, 2003

These examples are joined by a range of other legislative and policy directives in the United States, Canada and elsewhere, designed to ensure confidence and trust by mandating improved governance, oversight and adherence to best practices in both the private and the public sectors, including those related to privacy and security compliance.

Into the boardroom

As early as 2002, demands for good governance, regulatory compliance and the protection of corporate integrity resulted in the emergence of security as a key expectation. According to Michael Rasmussen, then director of research for the Giga Information Group, business partners and stakeholders' demands for security were becoming key business drivers. He stated: "Organizations are challenged to prove they are managing security to a level that will satisfy their business partners and stakeholders. This goes beyond discussing what security products are installed, to communicating compliance and management practices of information security."⁵

All of this has made security compliance a very real and highly visible responsibility for senior executives in both government and private industry. No longer is security solely a problem for technical administrators and network engineers—security has entered the boardroom and is featured in corporate audits and reviews. Surveys of major North American corporations over the past two years have consistently placed security and governance among the top 10 topics of interest for chief executive officers (CEOs), chief financial officers (CFOs) and chief information officers (CIOs). Specific issues within that context include:

- Security breaches
- Data protection and the risk of compromise of their own and partner/client strategic information
- Business continuity
- Compliance with privacy and other regulatory and audit standards

Security within enterprise management

In both private industry and government, executives at all levels are talking about governance, security directives and strategies. In government, the interest is particularly acute due to heightened national security concerns since 9/11. This interest is now being reflected in the direction that senior executives are issuing in the form of business drivers, strategic objectives and action plans. Although many of these organizations are still in the planning and policy phases, we are beginning to see funds allocated to address many of these issues—not in a piecemeal fashion, as sometimes occurred in the past, but in an approach that reflects a level of sophistication not commonly seen before in enterprise security. Senior executives are recognizing that the aggregation of increased governance, accountability and security demands a highly integrated approach that reflects basic business values and objectives and should be framed by an overarching strategy.

A business enabler

Consistent with reports from industry analysts, major organizations are seeking to implement a much deeper and more mature approach to security. Today, security is evolving as:

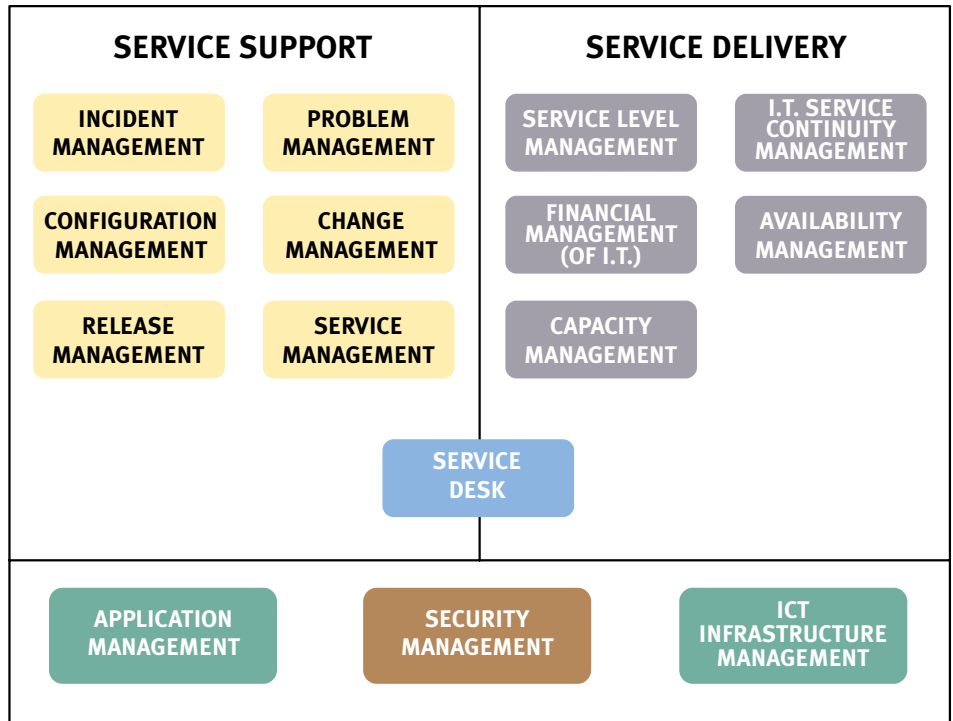
- A visible management responsibility
- A necessary and increasing component of regulatory compliance
- A complex set of integrated precautionary procedures, technical challenges, best practices and standards
- A way of managing risk, while still meeting the unending demand for greater connectivity and online services

With this more sophisticated approach, security is being forced to adopt new roles. No longer is it perceived as an impediment to open connectivity and technological exploitation. Instead, security is being recast as a mission enabler that no longer says "no," but advises "how" business and technological objectives can be prudently achieved, while staying within the bounds of policy and regulatory compliance. More importantly, security is finally being accepted as a major part of strategic risk management within the context of the preservation of business functions, integrity and asset assurance. Thus, in many ways, security has become both an executive responsibility and a mission or business enabler.

Emerging business-focused frameworks

As security becomes more tightly integrated with how IT services are delivered, corporate and government organizations are moving to a business-focused and cost-based IT service management framework. An example of such a framework is ITIL, which is quickly gaining popularity. Version 3 of ITIL formally recognizes security as a separate overarching process—separate from either service delivery or service support—and supports the entire IT Service Management framework. This approach (demonstrated in the following diagram) merely reflects the structure that many organizations have already begun to adopt.

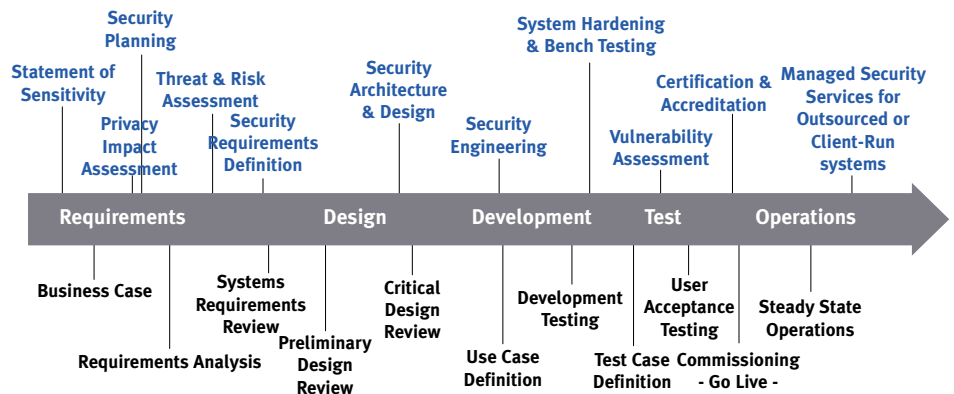
ITIL service management framework



Demonstrating the horizontality of security and the integrated nature of best practices, threat and risk assessments (TRAs), security certification and accreditation activities, as well as security audits should be closely tied to appropriate IT service processes, such as change, configuration and release management. These, in turn, are evolving as key, interdependent processes in the adoption of ITIL-based IT service management and enterprise management frameworks.

As in the case of configuration and change management, security also has a role to play in the development and delivery of new capabilities, specifically in the IT development process. The following diagram provides an example of the way that security should be tightly integrated into these activities.

Security elements in capability development and delivery

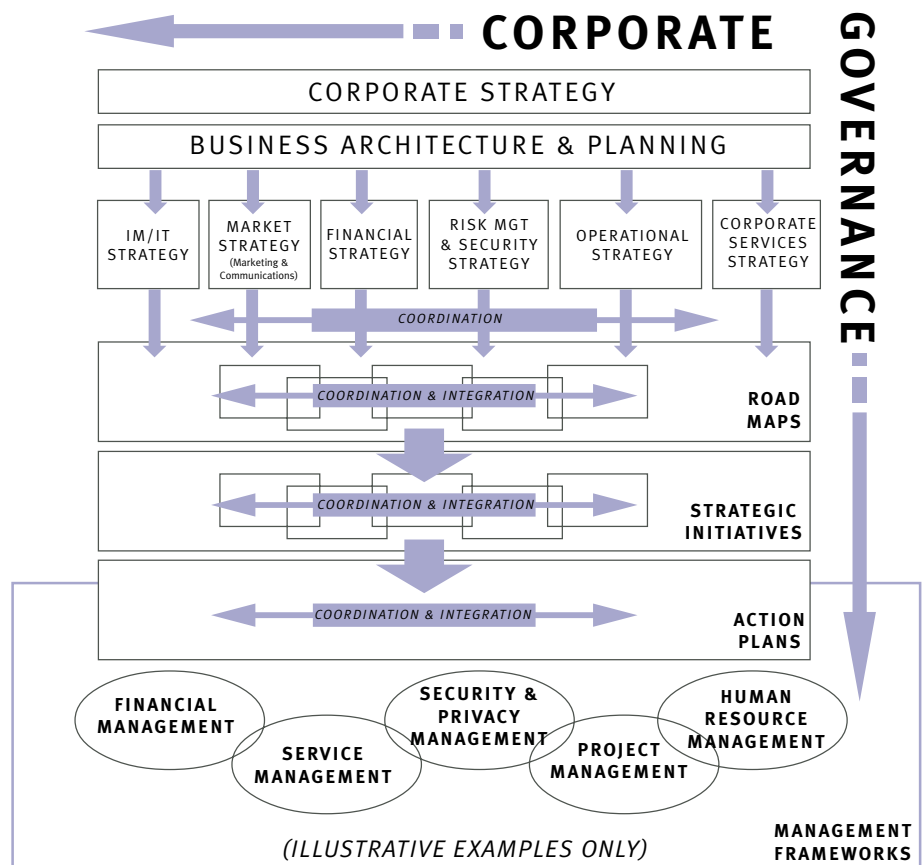


To ensure a successful security management implementation, there are several key recommendations to consider.

- View security as a management responsibility
- Create partnerships
- Avoid chasing fads
- Maintain balance
- Use frameworks wisely
- Integrate security from the start

Thus, what we see developing is an overall enterprise management approach that includes an IT service management framework, a project management framework (for new capability development), architecture frameworks and an increasingly mature and horizontally integrated security structure. Moreover, in some cases these various initiatives and frameworks are evolving into a comprehensive IT strategy that includes integrity, assurance and accountability as key foundation elements, with security as a principal means to this end. As previously noted, numerous private and public organizations have already introduced a number of security-related policies and directives to provide such strategic security guidance.

Relationship of security to typical enterprise activities



Elements of effective security management

Each of the principles discussed thus far are important. However, to ensure a successful security management implementation, there are several key recommendations to consider.

View security as a management responsibility—Security is now seen as an executive responsibility, essential to preserving an organization's vital business interests and to safeguarding the integrity of its reputation and assets. Security expectations begin at the highest level with investors, clients and regulatory authorities. It follows, therefore, that security must be consistently on the radar screen of senior executives.

Create partnerships—Increasingly sophisticated threats require equally sophisticated countermeasures. The days are gone when simply reviewing firewall and server logs and putting antivirus software on desktops was sufficient. Security is now such a complex and specialized field that it is impractical for most corporations and government entities to establish and maintain the level of expertise required in all its many facets. Now forensic and vulnerability specialists routinely evaluate IT infrastructure at the operating system, file system and code levels, while intrusion surveillance analysts regularly examine wire-based and wireless data packet contents, metadata and transaction protocols. Comprehensive SMTP and HTTP filtering are further evidence of the complex and varied risk environment in which we find ourselves.

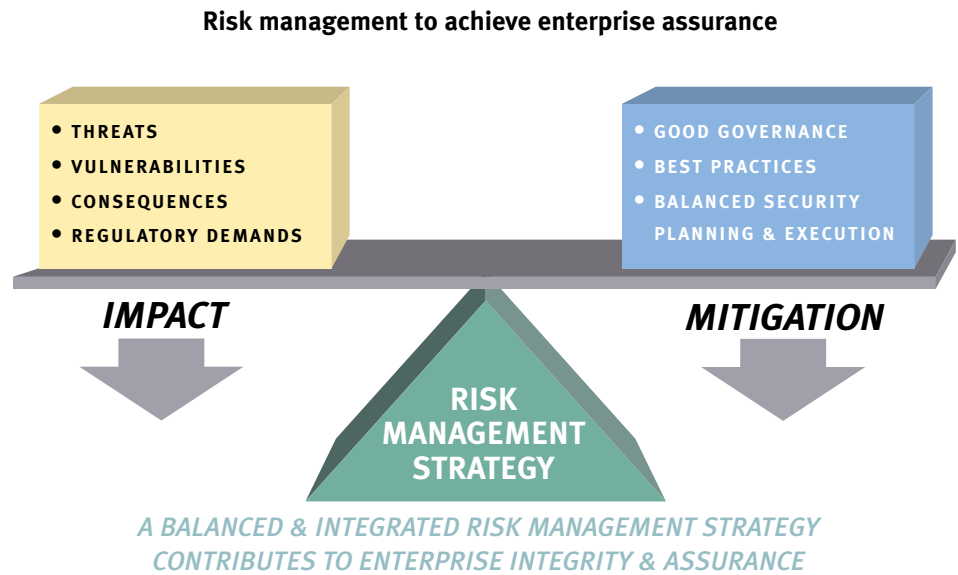
Acquiring these skills is difficult and the cost of maintaining and retaining skilled resources is high. As a result, many companies are establishing trusted relationships with expert industry partners, offloading risks and ensuring expert security services under comprehensive service level agreements. In addition to these private-sector partners, government departments and agencies are augmenting their expertise through security-related public-sector agencies, such as the Royal Canadian Mounted Police (RCMP) and the Communications Security Establishment (CSE) in Canada, the Computer Security Division of the National Institute of Technology Standards (NIST) in the United States, and the Communications-Electronics Security Group (CESG) in the UK.

Avoid chasing fads—Often times, many ideas touted as the "next new thing" in security are only new terms or spins for already well-established ingredients of a larger security approach. Nevertheless, their high visibility indicates current strategic interest and direction in government and private industry. The following are popular examples of "hot" discussion topics:

- Governance
- The creation of trust models
- Risk management at the strategic, operational and tactical levels
- Security audits and compliance
- Vulnerability assessment and management
- Defense-in-depth
- Identity management
- Anti-SPAM
- Anti-spyware
- Comprehensive managed security services, including intrusion detection and prevention and proactive antivirus management

Security is not a single dimensional problem. Therefore, any enterprise that relies solely on just one of these approaches for its security is not well protected. None of these, by themselves, is the magical and elusive security "silver bullet." Instead, each of these are building blocks in the larger and more comprehensive security structure needed to create and sustain a trusted business environment.

Maintain balance—Good enterprise security requires resources, diligence, common sense and, most of all, a clear realization by senior management that the integrity of their enterprise's infrastructure and the assurance of its assets are at stake. For this reason, a close and balanced relationship needs to be established between governance, best practices and security in order to manage risk and ensure that appropriate enterprise assurance levels are achieved and sustained.



© 2005 by CGI Group Inc. All rights reserved.

Use frameworks wisely—In addition to other benefits, best practice frameworks provide the structure and discipline necessary for sound security and the sustained achievement of business objectives. However, there can be "too much of a good thing." To that end, the following points are key:

- *Don't "collect" frameworks.* Framework overload can be a factor—management frameworks should be employed sparingly and deliberately. Too many overlapping schemes will cause unnecessary complexity and confusion, and may impose more risks than they prevent. Instead, choose the best management framework for your organization and its business model.
- *Avoid "process-for-process-sake."* Management frameworks and best practice schemes are based on process. Each will have purists—strict adherents that insist on a dogmatic approach to planning and implementation, often at the expense of practical goals and common sense. The successful implementation is lean and efficient. It will not break the principles of a framework, but rather will bend them slightly to accommodate key mission and business imperatives.
- *Don't organize to a framework.* Management frameworks are designed to provide guidance to an existing organization. They are not intended to act as an organizational model. Attempting to use them as such may result in a structure that does not fulfill your business needs. Make organizational changes only when they make clear business sense and use your management framework as a better way for people to do their jobs within a business-driven organizational model.
- *Don't hurry and take on too many concurrent activities.* Sound management is rarely built in haste. Instead it should be a deliberate and carefully executed process that includes evaluation, planning and training, and often a change in culture.
- *Don't expect to get it right the first time.* Plan to employ the Deming Wheel⁶, which involves planning, doing, checking (or measuring) and acting (or adjusting) at each step along the way. To this end, it's important to remember that management improvement is a continuous process.

Increasingly, organizations view the development and deployment of a comprehensive security roadmap as essential to the integrity of their enterprise. They are beginning to address security as an integrated horizontal supporting process and are looking outside their organization to trusted third-parties for solutions to their security challenges.

Integrate security from the start—Involve security planners in all aspects of enterprise planning, ensuring that good security exists by design and is tightly integrated into how the organization functions. This has the added benefit of ensuring that security principles have been designed to enable rather than impede key business functions.

Looking forward

Security as part of the executive team

The symbiotic relationship between governance, enterprise management and security is not merely a passing fashion. Information architectures continue to expand rapidly, providing ever more powerful capabilities while imposing exponentially increasing levels of complexity and significant challenges to management. Within this context, assuring an organization's integrity and the protection of its assets will become correspondingly complex, with effective security management at all levels seen as a key enterprise requirement.

To meet these challenges and to manage risk, organizations should tackle their security problem in four areas:

- Planning and strategy
- Design and deployment (often as aspects of larger projects)
- Day-to-day management activities
- Partners and supporting services

Increasingly, organizations view a sound security strategy and a comprehensive security roadmap as essential to the integrity of their enterprise. At a minimum, most organizations are placing security experience and expertise at the management level, thus providing strong guidance and leadership at the strategic/program level. With the current emphasis on greater accountability, there is a trend for corporate or departmental security officers to report to the chief financial officer, which allows close ties with corporate audit and review functions, or to the board or a designated executive committee. These trends are expected to mature and become standardized as the approach to governance and accountability consolidates.

Enterprise-wide security integration

Strong integration of security with all management frameworks throughout the organization, not just in IT, is expected to grow as organizations struggle with increasingly complex threats and growing demands for regulatory compliance, identity management and privacy protection. To this end, management frameworks will begin to more fully address security as an integrated horizontal supporting process. With the anticipated release of version 3 this year, ITIL will probably be the first. Security and management tools are also expected to begin to merge as they follow this trend, providing managers with an improved capability, such as in the use of dashboards, to establish and monitor key security metrics across an enterprise. This will allow more direct correlation between security and existing IT service management processes such as change management, the service desk and incident and problem management.

Partnering for strength

Collaborative partnerships, outsourcing and, when appropriate, insourcing are becoming an increasingly attractive and important option for many organizations. Faced with the need to protect the integrity of their enterprise and satisfy a growing range of diverse regulatory demands, corporate and government decision-makers are beginning to look beyond their own organization for solutions to these challenges. Many are discovering that by engaging specialist services risk can be reduced and efficiency improved at a cost that is often less than if the services were provided internally. Moreover, for those organizations that insist that their service providers meet best-of-breed criteria, problems associated with acquiring and

retaining highly qualified subject matter experts are taken out of their hands. Due to the economy of scale principle, a growing number of service providers are able to provide expert and experienced security services on a 24/7 basis, at a cost that is attractive to many IT budgets.

This trend is not unique to security, but rather part of a growing trend toward a more sophisticated hybrid delivery model in both government and private industry. In Canada and the United States, for example, three large federal government initiatives typify this move toward a broader, less parochial approach to IT services.

- **Secure Channel** is a portfolio of services that forms the foundation of the Government of Canada's Government Online (GOL) initiative, providing citizens and businesses with secure, private and high-speed access to all federal government online services. It also provides a common infrastructure that delivers secure and reliable network services for all federal departments, including a number of security-related services.
- Canada's **Shared Systems Initiative** was established to reduce the number of departmental financial, personnel and material management systems in use across the government and to achieve significant cost savings for these common processes. In this context, the government will act as its own outsourcer for a number of services. It can be expected that these services will be delivered to meet security, service management and regulatory guidelines.
- The U.S. Office of Management and Budget has launched the **Line of Business (LoB)** initiative. A major component of LoB is the requirement that federal agencies use Centers of Excellence (COE)—which consist of federal agencies, private-sector contractors or public-private partnerships—for IT hosting of certified software. Among COE requirements, a critical and central success factor is the secure management of this software as any deficiencies in this area will undoubtedly thwart LoB efforts to improve efficiency and performance.

In industry, there is a broad trend toward outsourcing. The data center and business process outsourcing market is expected to double over the next five years as businesses and, in some cases, government organizations seek to achieve cost and efficiency goals while managing risk and coping with growing security and regulatory demands. To be competitive in this rapidly expanding market, service providers will need to demonstrate that they can provide assurance that key business services will be sustained, data protected and corporate integrity safeguarded.

Conclusions

It is clear that security, enterprise management and governance are becoming inextricably linked. Whether in government or private industry, an organization's fundamental business strategy should be reflected in a governance approach that insists that sound security principals be integral to all business and service processes from the onset. This approach must also be visible at the executive level because, in the end, senior management will be held accountable for how they carry out their responsibility to protect the viability and integrity of the organization and its assets.

Based upon current trends, it is apparent that security requirements will continue to become increasingly complex, requiring a range of powerful solutions and trusted partnerships in order to meet diverse threats and growing regulatory demands.

Finally, managers at all levels must demand a security approach that empowers business objectives and is tightly integrated with all enterprise planning and management frameworks. This is perhaps our most important message for the future: Security must be seen as a fundamental management responsibility and an integral part of how we do business.

About CGI

Founded in 1976, CGI is a world-class leader in information technology and business process services. Through its focused industry expertise in financial services, government, healthcare, telecommunications, utilities, manufacturing, retail and distribution, CGI offers end-to-end services, including systems integration, strategic consulting, business solutions and the full management of IT and business functions.

Backed by rich heritage, global scale and a strong financial position, CGI has a solid track record of on-time, on-budget delivery and high-value repeat performance. Rooted in quality and management processes, its goal is to fully meet client objectives, serving as an accountable, flexible and objective partner.

To explore this topic and how CGI can help, contact your CGI account manager or visit 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.

Footnotes:

- ¹ - Source: 2005 E-Crime Watch Survey by CSO Magazine, U.S. Secret Service and Carnegie Mellon University Software Engineering Institute's CERT Coordination Center
- ² - Source: Media release 25 May 2004, CSO Magazine, U.S. Secret Service and Carnegie Mellon University Software Engineering Institute's CERT Coordination Center
- ³ - Source: CSO magazine's online feature "Analyst Reports," 21 August 2002: "Danger Within—Protecting your Company from Internal Security Attacks," by Richard Mogul, senior analyst, Gartner Group (<http://www.csoonline.com/analyst/report400.html>)
- ⁴ - Source: 2004 E-Crime Watch Survey by CSO Magazine/U.S. Secret Service/CERT Coordination Center
- ⁵ - CSO magazine's online feature "Analyst Reports," 18 December 2002: "IT Trends 2003: Information Security Standards, Regulations and Legislation," Michael Rasmussen, director of research, Giga Information Group (<http://www.csoonline.com/analyst/report721.html>)
- ⁶ - Deming's Quality Circle, commonly employed in ISO-9000 and ITIL methodologies, [see *IT Service Management: An Introduction Based on ITIL*, ISBN 90-77212-28-0, Information Technology Service Management Forum, (<http://www.itsmf.com>)]