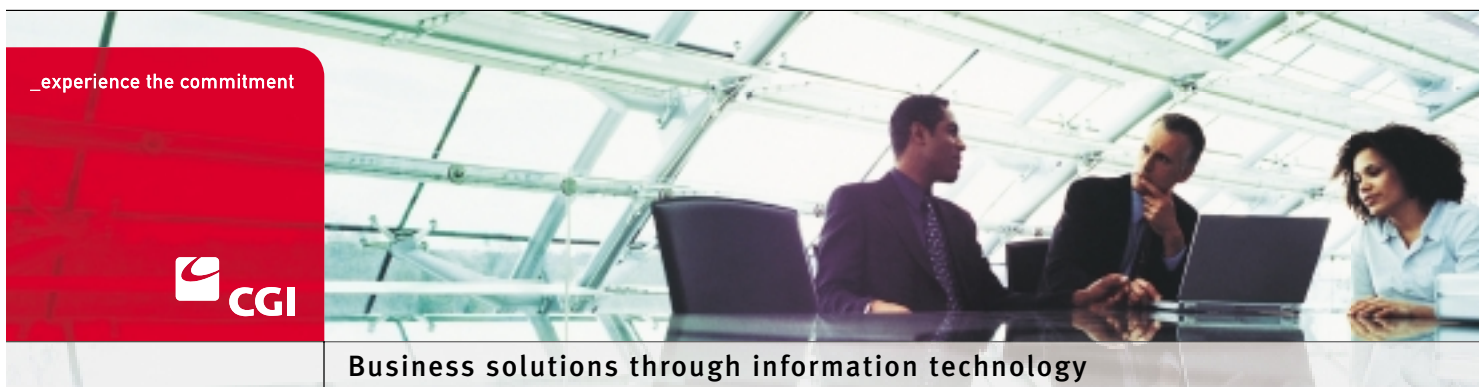


# Securing Critical Information Assets: A Business Case for Managed Security Services



Business solutions through information technology

## TABLE OF CONTENTS

INTRODUCTION	3
INFORMATION SECURITY DRIVERS	3
BENEFITS OF AN MSS APPROACH	4
CHOOSING AN MSS PROVIDER	5
CONCLUSION	6
ABOUT CGI	6

## Introduction

Information and the technology used to access, utilize, store, and transfer it have become the primary drivers of value and wealth creation in today's global digital economy. Businesses in every industry deal with massive amounts of information on a daily basis that must be protected from unauthorized access, vandalism, destruction, and theft. Likewise, the complex computer systems/networks through which this information is processed must be safeguarded. Failure to protect these valuable information assets can result in devastating consequences, including major financial losses and legal liability.

Within the last few years, the importance of information security has increased significantly due primarily to the proliferation of cyber crime and security-related legislation across the globe. Once a function relegated to the IT department, information security has moved up to the executive board rooms in many companies as a mission-critical initiative demanding serious focus and investment.

The increasing cost and complexity of information technology, however, have made the task of information security difficult for companies to manage on their own. As a result, companies are increasingly seeking outside help through Managed Security Services (MSS) providers. This white paper explores the benefits of MSS and what companies should consider in selecting an MSS provider.

## Information security drivers

### Cyber crime

The increasing risks and costs of cyber attacks are forcing businesses to take a much more aggressive approach to information security. Cyber crime is escalating at an alarming rate, victimizing people, businesses, and governments worldwide. While the Internet is revolutionizing communication and commerce, its open and ubiquitous nature has made computer systems and networks more vulnerable to internal and external attacks. Spanning the globe, the Internet has made it possible for a single cyber criminal to wreak havoc from anywhere in the world using only a personal computer and a modem.

News reports on the staggering damage caused by the latest computer virus or hacking incident have become commonplace. As society as a whole becomes more computer literate and new technologies emerge, the number of cyber criminals and the types of attacks they devise continue to multiply rapidly.

Although it is difficult to put an exact dollar figure on the costs of cyber crime on the world economy, it is estimated that the costs run into the billions of dollars every year. Cyber attacks impose both direct and indirect costs on businesses. Direct costs include money spent on security systems, programs and staff, as well as lost productivity due to security breaches. Although the indirect costs of cyber crime, including lost sales, damaged reputations, damaged customer relations, decreased shareholder confidence and legal liability, are more difficult to quantify, some researchers estimate they greatly exceed the direct costs.

### Security-related legislation

The threats posed by privacy and security breaches in cyber space have fueled an explosion in government legislation and regulations around the globe. Compliance, however, is an enormous challenge for companies due to the sheer number and complexity of these requirements. Worse yet, the risks of non-compliance, including fines, penalties, and negative media attention, can be very costly.

In the U.S., companies are impacted by a host of federal and state government mandates related to information security. Some of the more recent laws enacted include the following:

- **Health Insurance Portability and Accountability Act of 1996 (HIPAA)** - Requires health care organizations to safeguard the storage and transmission of electronic health information.
- **Gramm-Leach-Bliley Act of 1999 (GLBA)** - Governs the security of customer records at financial institutions.
- **Sarbanes-Oxley Act of 2002** - Imposes internal control and financial disclosure requirements on public companies.
- **USA Patriot Act of 2001, and the Homeland Security Act of 2002** - Implemented in response to 9/11, these laws establish information security requirements to guard against terrorist crimes.

Many other countries have likewise enacted security-related laws and regulations that companies need to be aware of and comply with as appropriate. In Canada, for example, the federal **Personal Information Protection and Electronic Documents Act** protects the privacy of personal information used for commercial purposes. In Europe, the European Union has implemented numerous privacy directives, including the **1998 EU Data Protection Directive**, which requires all of its member states to enact comprehensive legislation protecting the privacy of personal data.

International security standards have been developed to help organizations raise their level of security and comply with legal mandates. The most widely recognized security standard in the world today is ISO 17799, which evolved from its predecessor, the British Standard 7799. Developed by the International Organization for Standardization (ISO), ISO 17799 offers a comprehensive set of best security practices to guide executives in developing information security programs. More information about **ISO 17799** and BS 7799 is available at <http://www.iso.org>, or <http://www.bsi-global.com>.

### Benefits of an MSS approach

Companies face an uphill battle in their quest for information security. Threats to security continue to change and multiply along with the technologies used to deter them. Designing, implementing, and managing a successful security program is a vast, complex, and costly undertaking for most companies. Since no security program is 100 percent fail-proof, the success of a program is measured by its effectiveness in managing risk. Rather than assuming all of the risk/liability themselves, many companies are sharing the responsibility with managed security services (MSS) providers, and reaping a number of business advantages in return.

#### Cost

Cost reduction is probably the biggest advantage that companies achieve by outsourcing their security functions. In general, it is less expensive to outsource than to maintain a full-time security staff in house. MSS providers offer economies of scale by spreading out the cost for security experts, facilities, hardware, and software over numerous clients. In addition, the skills, experience, and advanced technologies offered by MSS providers substantially reduce the risk of cyber attacks, sparing companies the costs associated with those attacks.

#### Expertise

Due to the shortage of qualified information security professionals, attracting and retaining critical staff is a huge challenge for companies. Outsourcing relieves them of this

responsibility, leaving staffing in the hands of MSS providers. It also gives them access to highly trained and experienced security personnel. An MSS provider is able to recruit the best in the profession - people who have made information security a lifetime career - by offering training, career challenges, and promotion opportunities. Companies benefit from their professional certifications, technology know-how, and extensive experience in handling hundreds, or even thousands, of security incidences on a daily basis across many clients.

### **Facilities**

The facilities offered by MSS providers are another major outsourcing draw. Many providers have specialized security operations centers (SOCs) in multiple locations. Managed by highly trained personnel, these facilities are typically state-of-the-art, offering best-in-class hardware and software solutions designed to keep clients secure.

### **Service Performance**

Companies benefit from higher service performance levels by outsourcing their security functions to MSS providers. Through their security operations centers (SOCs), MSS providers can offer management, monitoring, and support services 24 hours a day, 7 days a week, 365 days a year, compared to in-house personnel who may only be available during normal business hours. Their operational procedures ensure uninterrupted service availability and fast responsiveness. In addition, through best practices and proprietary methodologies, they are adept at determining threat relevancy and eliminating time-consuming false alarms. MSS providers are also accountable for the quality of their services. Service levels are guaranteed, thereby, minimizing client risk.

### **Compliance**

Compliance with the myriad security-related laws and regulations existing in most countries today is a daunting task for businesses. Not only must they understand the intricacies of these complex legal requirements, but also come up with solutions for bringing their security programs into compliance. Through MSS outsourcing, companies gain access to compliance expertise and solutions. MSS providers offer comprehensive knowledge of legal requirements and industry standards, as well as experience in developing and implementing best security practices. They also provide audit services to ensure clients remain in compliance on an ongoing basis.

### **Choosing an MSS provider**

Choosing the right MSS provider requires careful planning and deliberation. The MSS market is saturated with vendors whose services, skills, and experience vary widely. Many vendors either lack the services and solutions that you require, or what they offer is too generic to address your unique needs. Make sure you specify your security requirements up front, and ask prospective vendors to clearly demonstrate their ability to meet those requirements. Additional considerations in selecting a vendor include:

- **Financial stability** - Does the vendor have a strong balance sheet? Does it have a history of strong financial performance and a diverse client base?
- **Security services** - Does the vendor offer a wide range of security services to address your end-to-end security requirements? Is it willing to package those services in a way that best suits your particular business needs? Can its services be scaled to your future growth?
- **Expertise** - How large is the vendor's staff? Does it offer training programs? Is its staff certified? What are the staff's average years of experience?

- **Security operations centers (SOCs)** - How many SOC's does the vendor operate, and where are they located? What types of technologies do they leverage? Are their operational procedures well documented? What security management methodologies do they use? How often are their systems audited and by whom?
- **Industry/quality assurance standards** - Does the vendor comply with international and national security industry standards? What quality assurance standards does it follow? Does it belong to standardization organizations? If yes, which ones?
- **Customer support** - How many clients does the vendor currently support? How many security incidences does it handle each day? What are some examples of recent incidences, and how were they resolved? Does the vendor offer current and past client references?
- **Service level agreements** - Does the vendor offer clearly defined service level agreements? Do these agreements provide for built-in flexibility? Are there stipulated penalties for non-compliance? Is there a confidentiality provision?

When choosing a vendor, a company should strive to build a good working relationship founded on mutual trust and respect. Strong communication is essential for building this type of relationship. Some companies have a tendency to leave security completely in the vendor's hands, taking an "out of sight, out of mind" approach. A better approach is to assign one or more staff members to stay on top of pressing security issues, and oversee the outsourcing relationship to ensure risks are effectively mitigated and contractual obligations are fulfilled.

## Conclusion

A "good enough" security program is not good enough in today's volatile security environment. Putting in place a second-rate program can result not only in major business losses, but ultimately business failure. The increasing complexity of security requirements and solutions is driving increasingly more companies to consider managed security services (MSS) outsourcing. Those who have pursued this strategy are experiencing a wealth of advantages by leaving security in the hands of experts, and re-focusing their attention on their core business.

With the largest information security practice in Canada, CGI is at the forefront of MSS. Through our security centers of expertise, we deliver a full suite of security services, designed to address our clients' end-to-end security needs. For more information on CGI's MSS capabilities, visit our corporate Web site at [www.cgi.com](http://www.cgi.com).

## 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](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](http://www.cgi.com)