

Securing Important Information Assets

Guidelines for Small and Mid-Size Business

by Claudiu Popa, CISSP, PMP, CISA
President, Informatica Corporation
InformationSecurityCanada.com
Information Protection Since 1989

1. Introduction

In the opinion of the informed security industry as well as that of most governments, 2006 is the year when information security finally arrives at the forefront of business priorities. This is due to three factors:

1. attacks against companies of all sizes to increase in severity
2. financial losses are expected to be at least 50% greater than last year
3. awareness and understanding of the threat increases among managers

The last point is of particular importance. Managers and business owners are beginning to understand that:

1. their valuable information is at risk, and its compromise can mean loss of business, loss of customer trust and loss of money.
2. increasing regulations are putting pressure on businesses to be compliant with privacy, confidentiality and security laws
3. security is not a subset of their IT staff's skill-set but a distinct discipline that must be exercised by independent experts
4. information security can have a positive impact on profits and business growth

2. Benefits

Indeed, beyond protecting a company's information assets, a strong security strategy will boost business by:

1. helping to differentiate the company and showing competitiveness
2. establishing trust by showing an emphasis on protecting client assets
3. demonstrating added value through investments in privacy protection, secure communications and awareness, regulatory compliance
4. showing an understanding of security in every aspect of the business: human resources (secure hiring practices and privacy), marketing (compliance and PR), governance (leadership and management), corporate training (employee security awareness), information systems (IT security, networking, etc), e-business (website and database security), etc.

3. Key Points to keep in mind when determining the need for information security:

1. Does the company collect and store any client information? (of course)
2. Do any laws and regulations apply to its protection? (in Ontario, yes)
3. Does the company depend on computer systems and files to store financial, client, transactional and backup data? (of course)
4. Are workstations connected to the Internet? (most likely)
5. Does the company have a Web presence? (most likely)

This establishes the existence of the 4 areas of small business information risk: Systems, Communications, Storage and Web. For **any** small or mid-size business to properly manage its security, the following must be true:

1. all computers (workstations, laptops and servers) must be hardened and secured to protect against security threats
2. security products must be installed and configured by trained experts to ensure effectiveness
3. web site functionality, data storage, backup and communications practices must be audited and secured to protect privacy, confidentiality and integrity.
4. management must implement a strategy for on-going security assessment and periodic check-ups by qualified experts
5. written policies must be communicated to staff to raise awareness and educate employees about risk and best practices.

4. Why Informatica

Informatica has protected the information assets of businesses of all sizes since 1989 and can satisfy these requirements better than any other company by:

1. using the expertise of experienced, certified professionals
2. applying industry-leading security analysis tools and techniques
3. selling and installing world-class products and solutions
4. providing support and regular maintenance for security management
5. teaching employees the basics of information protection and secure Internet practices

Informatica's reach include expertise in research, training and consulting along with the provision of layered security and risk management. The company's offerings are the most comprehensive in Canada and are carefully crafted based on client needs and expectations.

5. Approach, Process & What To Look For

Discussing information security is simple. Every computer user today is experiencing its effects. These include identity theft attacks through spam, viruses, worms, spyware, data loss, concerns about internal theft, issues regarding proper protection and installation, business continuity and data recovery, etc.

Most companies realize that they are unprotected but hope that the issue will disappear by simply ignoring it. It is easy to determine preparedness by simply addressing the Key Issues mentioned above with the following questions:

What to look for:

1. Is every computer system secured by software and configuration changes to make it impermeable to security breaches and malware? This is above and beyond anti-virus software and any corporate firewall.
2. Is the corporate privacy policy a reflection of current practices, implemented software controls and compliant with the current privacy law?
3. Are computer systems connected to the Internet?
4. Is there a specific review of security (logs, updates, software, protection) performed every 2-3 months?
5. Has the company Web site been checked for security vulnerabilities? What about the corporate network and the backup system?
6. Are security tools, software and network components installed by security professionals or just the local IT staff?

The answers to these questions typically indicate a need for the company to adopt the following services:

1. policy review, web site assessment, network and technology implementation review
2. privacy compliance and best practices audit
3. monthly security check-ups and support plan
4. staff security awareness seminar
5. systems hardening and lockdown

But before that happens, Informatica can produce a detailed report of the current 'security posture' of the company and give management a clear picture of what needs to be done on an on-going basis to preserve the security of information assets. All pricing is provided as a flat fee and covers specific aspects of security management, not interfering with the functions of existing IT personnel and other professionals.

Introducing Informatica

"Does anyone provide your organization with security support for all aspects of data security?" The answer to this question is invariably negative since IT staff are not traditionally security experts nor do they want the added responsibility. Product vendors have no interest in offering this type of support, so a meeting with Informatica or a business security assessment is always a worthwhile exercise.