



- LOUIS J. CARPENITO CISM, CISSP -

A Virus of a Different Kind: Internet Security and Canadian Healthcare

Mr. Carpenito is the Vice President, Information Security Business Strategy at Symantec Corporation; he is an expert in privacy and security regulatory requirements for the healthcare and financial industries.

The Internet has spurred a profound change to the meaning of the word virus. Yet with the push toward a Canadian “eHealth” system, computer viruses and those that have plagued humans for centuries have merged into the same arena. Last year’s Commission on the Future of Health Care report highlighted the need to take full advantage of the potential information, evidence and ideas in the health care system through information infrastructure. Putting the essential information management and technology systems in place will ensure that essential information can be collected, compiled and used to make better decisions and improve quality and care within the public health system.

Canadian healthcare institutions currently spend only 1.8% of their budgets on IT.¹ But things are changing; Canadians are increasingly viewing technology as an important pillar of the healthcare system. The movement towards electronic health records is a clear example of a technology advance that is changing healthcare. In fact, the implementation of Canadian electronic health records is already underway. Entitled the “eHealth” system, these electronic records promise to give healthcare providers immediate access to accurate and timely information that facilitates informed decision-making and helps to extend patient care into the community and home. While these advances are exciting, proper security safeguards including policies, processes and tools are required to ensure the confidentiality, integrity and availability of sensitive personal health information (PHI).

The realities of today’s e-world are apparent, especially as they pertain to the security of highly confidential health-related information. Security threats are increasing and organizations across the board are fending off viruses, worms, malicious code and cyber attacks on a daily basis. In fact each week, more than 100 new viruses are identified and nearly 70 new software vulnerabilities are discovered. New cyber attacks that use blended threats, combining hacking, denial of service, and worm-like propagation, makes the cost and impact of these attacks more damaging than ever.

Code Red and Nimda are good examples of this. Code Red had an estimated worldwide economic impact of \$2.62 billion and Nimda’s estimated economic impact was \$635 million. While Code Red and Nimda have stolen the spotlight, the Klez virus has quietly been becoming one of the most persistent viruses of all time. Six months after the virus was first detected Symantec was still receiving more than 2,000 reports of new infections a day. SQL Slammer illustrated the evolution of worms by becoming widely acknowledged as the fastest-spreading worm yet seen. More recently the Blaster and Welchia worms and the SoBig variant (SoBigF) kept IT professionals on the alert for several weeks.

With the advent of mobile computing, wireless LANs and the expansion of business partner connections for portability it is difficult to establish static perimeters around the entire network. Our perimeters have become dynamic and therefore new security techniques are required.

But as security threats become more complex, demands on the healthcare system are growing. There are increasing expectations from patients and stakeholders who want improved service and secure access to their personal health information. Not to mention the regulatory requirements that are getting more complex and demanding.

In this climate, the Canadian government is addressing the protection of personal health information on all levels. The federal, provincial, and territorial governments have developed a combination of legislation, policies, regulations, and voluntary codes of practice. Some of the federal legislation includes the Access to Information Act, the Personal Information Protection and Electronic Documents Act (PIPEDA), Privacy Act, and the Statistics Act. In addition, many provinces/territories have legislation protecting personal information in the public sector. By January 1, 2004, the PIPEDA will apply to personal health information (including patient health services information, registration and practice information of health professionals and institution-identifiable information) collected, used, or disclosed in the course of commercial activities within a province/territory that does not have “substantially similar” legislation.

Government regulations are an important step toward securing confidential patient information enforcement however, can be problematic. For example, PIPEDA is highly dependant on “whistle blowers.” Individuals may file complaints with an organization or directly with the Privacy Commissioner. Once the complaint is deemed to have reasonable grounds, an investigation will be launched. The Commissioner may also initiate an investigation or audit without a complaint using the Commissioner’s broad investigatory powers. To date, the Commissioner has been reluctant to do this.

Regardless of how investigations are initiated, they can result in the publication of a report containing the results of the audit or investigation. As a result, the primary risk of violating PIPEDA is the negative publicity generated from a Commissioner’s report - not to mention the potentially unlimited financial damages in federal court.

Yet as the government develops appropriate legislation and methods of enforcement to protect patient information, most healthcare organizations are trying to address their security needs with constraints on time, budget and personnel. Information

“...the best way to protect sensitive health related information against any particular threat is to know about that threat or the vulnerability it exploits before it hits. An alert system should provide you early warning against threats and actionable information on how to protect against an attack.”

security is often not a core competency of today’s businesses and IT budgets are not always in line with security requirements.

Addressing today’s complex security challenges and the requirements contained within Principle 7 (Safeguards) of Schedule 1 of PIPEDA requires a holistic security strategy that must be integrated with the overall healthcare administration strategy to be truly effective. A holistic security strategy must comprise of at least four of the following critical elements including:

1. Risk assessment and analysis
2. Risk management strategy
3. An alert system that provides early warning against threats and vulnerabilities
4. A system that protects PHI against loss, theft and unauthorized access, disclosure, copying, use or modification
5. The appropriate level of security controls (technologies) across all tiers of the infrastructure to protect critical systems, applications and information

6. A plan in place to respond to a security incident (attack, unauthorized access, etc.)
7. A comprehensive security architecture and system to manage the ongoing process of securing your infrastructure and information

Conducting an accurate and thorough assessment of the potential risks (threats and vulnerabilities) to the confidentiality, integrity, and availability of electronic protected health information is essential to protecting sensitive health related information. This assessment should include potential malicious and/or accidental disclosure, misuse or modification of electronic protected health information, and the potential malicious and/or accidental misuse and/or modification of sensitive healthcare technology.

The inventory of healthcare technology and electronic protected health information should be the focus of this risk analysis. In addition, any security monitoring, protection and detection mechanisms that have been deployed must be assessed as well.

Tired of Spam?

- Gartner predicts that by **2004**, unless an organization takes defensive action, more than **50%** of corporate e-mail message traffic will be spam
- **67%** of email administrators said the increasing volume of spam is an overwhelming, major or notable problem
- **49%** of end users said they received 10 or more spam messages **per day**
- **Spam reduces productivity** and exposes organizations **to legal liability**

UNIS LUMIN recommends NetIQ Marshal content security products to control spam, detect viruses and reduce legal liability.

Visit us at www.unislumin.com and register for NetIQ’s in-depth white paper entitled: "Controlling Spam". Learn about the growing problem spam is causing organizations and how you can use policies and technology to control it.

UNIS LUMIN
TECHNOLOGY-BASED BUSINESS SOLUTIONS



The risk assessment should be conducted from an end-to-end perspective. An example of an end-to-end perspective is following the electronic protected health information flow from its entry points through business system applications, hand-held devices, workstations, servers, databases, network devices and internal and/or external networks to its final destination(s). Particular attention should be made to the access, storage and transmission of this information.

Additional steps beyond the electronic protected health information are required for sensitive healthcare technology. In this case, the organization will also need to assess both access and internal controls of the technology. It is highly recommended that they involve safety personnel to understand the potential risks of death and/or harm to the patient, through accidental and/or intentional electronic misuse of this technology.

The results of the risk assessment process should identify all of the risks including: the affected assets (technology and/or electronic protected health information), the level of severity and level of probability of misuse, unauthorized disclosure or exploitation.

Determining what steps will be taken to manage the risk(s) that are identified through the risk assessment process and/or reported through other channels is a key step organizations must take. There are several strategies that can be adopted: eliminate, mitigate, insure and/or accept the risk(s). An organization's risk management process should include a consistent approach in making the risk management decision. It should also recognize the existence of privacy and security best practices and standards, security protection and detection technologies and, threat and vulnerability early warning and response capabilities.

Without a doubt, the best way to protect sensitive health related information against any particular threat is to know about that threat or the vulnerability it exploits before it hits. An alert system should provide you early warning against threats and actionable information on how to protect against an attack.

A security partner that is tracking threats and vulnerabilities around the clock can help a healthcare organization understand

- What new threats are emerging
- What vulnerabilities are most likely to be exploited in your environment
- What defenses you need to implement to prevent an attack

Having a security partner that customizes its alerting system and evaluates every vulnerability is a key component of effectively prioritizing which are most critical and need immediate attention.

Putting an early warning system in place is the first step. Next, organizations need to make sure to protect their business systems, process and critical data. The Internet has enabled healthcare organizations to share information, transact business and communicate with partners, employees, doctors and patients online. Yet, with the number of threats increasing, these points of entry become opportunities to attack a network.

Integrated security implements solutions at the gateway, server and client levels. It brings together key technologies such as antivirus, firewall, intrusion detection, VPN and vulnerability management into one seamless solution, providing better protection against today's blended threats like Code Red, Nimda or Klez. This type of integration enhances security and manageability while optimizing performance and return on investment.

The integration of the technologies allows the client firewall to

instruct the antivirus and intrusion detection engines to scan all outgoing files. If a threat is detected, the antivirus or intrusion detection engine can then instruct the firewall to increase security measures and block the file. It will alert administrators to potential threats through a common console and contains the threat within the client, preventing the infection of the entire network.

Integrated security solutions enable centralized configuration, deployment, installation, and policy management. This approach helps reduce the overhead, risk and administrative headaches that are common with disparate point products from multiple vendors. It also eliminates interoperability issues and simplifies the security environment.

Once an organization is alerted to potential threats and you have the necessary solutions in place, organizations also need to be able to respond in case of an attack. A response plan must start with intelligence about the attack; countermeasures to address it and details on how to clean up any damage ... whether a healthcare organization chooses to manage their own environment or have an Internet security provider do it for them.

Effectively protecting against increasingly complex threats requires a combination of technology and expertise aimed at streamlining security through early-warning systems, powerful solutions, and automated response. All of this must be tied together under an open, comprehensive, standards-based management system that spans all tiers of the network and runs on multiple platforms. Without such a system, the process of aggregating and normalizing security-event data is inefficient and difficult, which, in turn, makes effective protection nearly impossible.

Security now requires the attention of healthcare administrators and the board of directors. Executives are accountable to patients, employees and suppliers. Taking the lead to establish safeguards to protect security, business continuity, and privacy is the responsibility of top management. To do this, management must establish a security policy committee that includes the CIO, CISO, HR, IT, facilities and legal. This multi-department team will be responsible for the design, development, implementation and enforcement of a corporate-wide information security program.

Finally, a sound security program also includes education. Employees need to understand the organization's security policies, their security responsibilities and how to make security part of their daily activities. Many companies offer security awareness programs and training and certification classes.

A proactive approach to security is key. It's important to view security in the same light as insurance. Investing in a secure environment today ensures protection from tomorrow's threats and compliance with security and privacy regulations.

¹ Canada Health Infoway Inc., Infoway's EHR Pan-Canadian Survey, January 2003, <http://www.infoway-inforoute.ca/pdf/EHR-Survey-Phase1.pdf>

