Trust Systems for Regional Healthcare

Andrew Matthews

In every healthcare setting, there is an expectation of privacy and security. Patients expect their records to be confidential, and the healthcare provider is responsible for ensuring that this is the case. Until recently, this has not been an issue as records have been paper based and kept in files under lock and key. But with the move toward creating standard electronic health records that can be shared across multiple institutions and by greater numbers of healthcare professionals, the potential for a privacy breach increases exponentially.

The creation of regional health organizations such as Regional Health Authorities (RHAs), Local Health Integration Networks and Regional Health Information Organizations is adding to the complexity of the security issue. As the arbiters of funding decisions, these organizations have developed and implemented accountability and performance management agreements with local providers to improve the way healthcare services are planned and delivered within their region. Groups between providers are being created to streamline operations and demonstrate cost savings across the board in order to be eligible for the funding of new initiatives. This requires complete sharing of information across the group, opening up new avenues for risk. The result is that more sophisticated security solutions are required.

This profile is about one RHA; composed of eight healthcare facilities including research and teaching hospitals, general and acute care facilities and long-term care providers, it was created to serve a combined community of approximately one million people. Beginning in the late 1990s, the hospitals embarked on regional collaboration to create a shared hospital information system and a regional picture archiving and communications system. With these key steps completed, they were ready to establish integrated electronic healthcare between facilities.

In order to achieve a truly integrated e-health system, it was critical for the member organizations to establish a deep level of trust in each others' capabilities and commitments to protect patient information.

Understanding that security would be a critical component of the project, the group turned to its attention to developing a comprehensive security strategy. In order to achieve a truly integrated e-health system, it was critical for the member organizations to establish a deep level of trust in each others' capabilities and commitments to protect patient information. To establish a foundation for this trust, the hospitals decided to implement a regional security strategy to uphold the integrity, quality and confidentiality of patient information.

The regional security strategy reinforced the group's desire to maintain current protection for data integrity and system availability while increasing the region's ability to ensure the confidentiality of clinical data in accordance with local regulations such as the Personal Information Protection and Electronic Documents Act, Ontario's Personal Health Information Protection Act and the Healthcare Insurance Portability and Accountability Act. The secondary goal was to create a more efficient security system that could be embedded into operational practices (managed via metrics), enabling the region to capitalize on economies of scale by standardizing on products or implementing shared services.

Hospital Security: Who's on First?

Each of the eight participating hospitals had varying levels of security and disparate systems to manage this critical function. Security was the responsibility of the individual information technology (IT) departments and, as such, was not a tracked feature within each organization's portfolio. With the advent of new privacy laws and the increased focus on security measures to ensure adherence to these laws, the IT departments realized there was a great deal more they could do in this area. The challenge facing them was to set a standard for security across the group so that each hospital felt comfortable sharing its information while allowing individual IT departments to maintain their autonomy for managing their operation.

The regions adopted a three-year road map for achieving the group's goals, including the following:

- An enterprise-by-enterprise security assessment based on International Standards Organization (ISO) standards
- Documentation and publication of the region's Security Strategy and Operational Security Plan
- The implementation of key security program elements, including an executive security scorecard for initial and ongoing measurements of security posture, event correlation and response, security awareness, compliance and technical security measures

To achieve the desired level of trust, the region conducted an audit and assessment to analyze and understand the security risks common to each facility. The hospitals agreed to adopt a

This project profile supported by education grants from Emergis.

modified version of the ISO 27001 standard for security management. An assessment of each facility took place documenting the technology infrastructure, systems and processes currently being used to manage security. A risk profile was created by applying the proven structure of military organizations as the foundation for their security strategy. The profile became a benchmark to establish a common understanding between organizations as to exactly where they were and what they had to do together to achieve the level of security required.

The overall security strategy for implementation was developed for the group and included a number of elements that were categorized into four strategic areas: (1) security management team structure, (2) policies and standards, (3) enforcement and measurement and (4) operational security. These areas made up a regional security management framework. The framework defines a set of information security controls and takes into account a regional perspective rather than being location specific and technology or solution focused.

The key to success for this program is the ability to centrally track performance.

Security Strategy: Organizational Recommendations

To be effective, the responsibility for the implementation and management of the framework had to reside in a centralized organization. A modified Federated Information Risk Management Organization was implemented. This organization is spearheaded by a regional information security officer (RISO), who oversees the creation and maintenance of shared security elements such as the overall strategy, policies, enforcements, compliance and a regional incident response capacity. The RISO is the central point of communication and coordination within the region, managing the budget and ensuring an equitable allocation of costs among the hospitals. The creation of the federated structure builds on the existing leadership, solutions and assets within each of the hospitals and helps to foster collaboration, sharing and reusing of solutions throughout the region.

Each hospital within the group also adopted the recommendation of a formally recognized information security officer to work with the regional body rather than report into it. The role of information security officer is a crossover staffed by a senior person within each of the member hospitals. Working with local IT teams, privacy groups and other organizations, the information security officers lead all aspects of security implementation and management within their specific hospital.

The security program also called for the development of and adherence to common security policies, standards and guidelines to establish the ground rules and standards under which the organizations would operate their information systems. Underlying each specific policy is the common goal to reduce the risk of, and minimize the effect or cost of, security incidents.

Enforcement and measurement program elements were designed to collect data on critical systems, to analyze key indicators for security and privacy management and to provide meaningful feedback via scorecard reporting, compliance reviews and assessment reports. The key to success for this program is the ability to centrally track performance. Data are provided directly to the RISO as required to perform both pre-deployment assessments and regularly scheduled compliance reviews. A Centre of Excellence network laboratory is scheduled to be built to support the enforcement and measurement requirements throughout the region. This isolated environment will be created to test the overall security of proposed products and solutions. The laboratory will benefit all hospitals by providing access for all sites to standardized hardware and software configurations that have been tested against critical applications.

Security Strategy: Technical Recommendations

Even with policies, procedures, enforcement and measurement criteria, the security program would be moot without operational activities to provide the technology backbone on which it is based. The organizations identified several areas that required attention, including the following:

- Network control and segregation
- Centralized log management
- Intrusion prevention services
- Security compliance management suites
- Security operations centre
- Development of shared services
- Account management
- Vulnerability management
- Security incident response capabilities.

They subsequently adopted a security compliance management suite as opposed to individual tools to address the group's technology requirements. With a suite vendor, the hospitals were able to take advantage of many inter-related tools at a low cost; have access to an array of security tools quickly; leverage more support options and a higher level of service from the vendor; take advantage of best practices across the region with a common skill set; and lower overall training and maintenance costs. Existing applications, where appropriate, were integrated with the security suite to leverage best practices across the organization and provide additional cost savings. This intelligent integration of technologies set the standard for security across the region. Additionally, by adopting best-of-breed and point solutions for the group, the RISO now has access to regional reporting from a standard suite of products.

This project profile supported by education grants from Emergis.

Changing Rules, Changing Behaviour

In any organization, security must take into account the people who actually use the systems. The most well-intentioned, sophisticated and advanced security initiatives will fail if people do not adhere to procedures, adopt the standards and processes or carry out job functions effectively as intended.

With eight hospitals and thousands of people accessing the systems, achieving buy-in and support for new security measures is a critical factor for the hospitals. As the group moves forward in their three-year plan, the intention is for a change management program to be developed and deployed alongside the operational security plan to ensure the successful adaptation to change required. This will encompass the delivery of meaningful and timely communication to various stakeholders, the active engagement of stakeholders throughout the process to solicit input and expertise and the education and training of all hospital personnel to ensure minimal disruption and the quick adoption of new security measures.

Emergis supported the development of this regional strategy and is also providing the hospital group with transition support and knowledge transfer. Using a variety of tools such as knowledge bases, help desks, document management and content management systems, this will ensure that the group acquires the appropriate knowledge and skills to successfully maintain and manage security in the region going forward.

The ultimate goal for the regional hospital group is to achieve a sustainable, efficient security program that is virtually invisible to employees.

The ultimate goal for the regional hospital group is to achieve a sustainable, efficient security program that is virtually invisible to employees. It should result in a dramatic reduction in security incidents and response times. Security is in compliance with strict Ministry of Health legislation and Canada Health Infoway standards. And, finally, the security program must allow the vital development of the shared electronic health record for the region to continue without any security roadblocks. This will be modern healthcare management.

About the Author
Andrew Matthews is Director Of Security Services, Emergis Inc. and can be contacted at andrew.matthews@emergis.com

This project profile supported by education grants from Emergis.