



- BRANTZ MYERS -

Lakeridge Health's Multi-Site Security Deployment Ensures a Healthy Network

Brantz Myers is the Enterprise Marketing Manager for Cisco Systems Canada

"With our upgraded network security our staff, partners and patients can feel confident that communications and data are highly protected from outside intrusion or malicious events."

- Deborah Anthofer, director, Information Technology, Lakeridge Health.

Background

Around the world, healthcare organizations are building integrated networks in order to amalgamate services, share resources and enable access to improved services for patients regardless of location. Lakeridge Health is one such organization. Located in Ontario, Canada's most populous province, Lakeridge Health serves several communities in the suburban Toronto area.

Lakeridge Health is anchored by four hospitals in Bowmanville, Oshawa, Port Perry and Whitby, Ontario. It also connects 17 other local services including physiotherapy, dialysis and rehabilitation centres, addiction centres, clinics, ambulance and some physician offices. One of Ontario's largest hospital networks, Lakeridge Health delivers healthcare services to more than 500,000 people in rural and urban communities in the fast growing Region of Durham.

The hospital's mission is to work together for excellence in healthcare, to collaborate with its partners in the promotion of health and well being, and to undertake continuous monitoring and improvement.

Challenge

Recently, much of that focus on improvement has been directed at strengthening Lakeridge Health's network security, especially as it connects to the Smart Systems for Health Agency (SSHA) network. SSHA, a publicly-funded project which is part of the Government of Ontario's e-Health Strategy, is providing a secure, integrated, province-wide information infrastructure to allow electronic communication among Ontario's healthcare providers. More than 80 per cent of Ontario's hospital networks are now connected to the SSHA network and once fully operational it will connect more than 150,000 healthcare providers across 24,000 sites throughout the province.

In anticipation of the upcoming connection to SSHA, and as part of their continuous mandate to update security, Lakeridge Health determined they needed some significant security upgrades.

"We had only a single point of protection, through a solitary firewall. No real-time monitoring, no protection against third-party or dial-in connections," says Deborah Anthofer, Director, Information Technology for Lakeridge Health. "We needed to upgrade our total network security."

In 2001, Lakeridge Health engaged Deloitte's IT security services practice to conduct a comprehensive security audit. The audit recommended Lakeridge Health implement an integrated security strategy, including real-time security network monitoring and intrusion detection.

"Lakeridge Health needed a solution that would provide its partners with secure, scalable connectivity and remote access. They wanted an infrastructure for third-party connectivity, and a solution that was cost-effective to ensure a return on investment," says Mike Bronson, senior manager of Security Services for Deloitte.

Solution

Deloitte recommended a multi-tiered security solution that incorporates a system-level approach to deliver secure connectivity, threat defense, and identity/admission control. Based on Cisco firewalls, virtual private networks and intrusion detection, the integrated, end-to-end security solution protects the network infrastructure and critical endpoints, controls access and protects external communications.

"We built a new network architecture to provide and maintain confidentiality and integrity from storage to transmission across Lakeridge Health's sites," explains Rejean Loisel, Manager of Technical Services, Information Technology for Lakeridge Health.

The solution includes a second layer of defense through a second set of firewalls, intrusion detection, plus "De-Militarized Zones" (DMZ), or isolated areas on the network between two firewalls for state-of-the-art security. The DMZ concept incorporates an anti-virus gateway, a remote dial-in server, and Web filtering and monitoring. The solution also includes a central management console at the Oshawa Hospital-based corporate data centre for real-time monitoring.

Instead of creating one major DMZ, the solution uses the firewalls in a multi-tiered approach to effectively provide a series of DMZs for various types of communication based on different levels of trust. All the hospital facilities are connected together, and to SSHA, by utilizing these different DMZs. The "trusted" DMZ enables secure communications between Lakeridge Health's affiliates; the "untrusted" DMZ is for communication with the public.

Lakeridge Health uses Cisco PIX firewalls to protect the network "edge" - the point at which the internal network connects to the outside world. Cisco PIX firewalls are installed at each the four central locations, and at each of the 17 Lakeridge Health off-sites and other services locations.

To further protect the data and information infrastructure, Lakeridge Health uses the Cisco Intrusion Detection System. This software analyzes network activity, detects security breaches, then automatically sends alerts to administrators and reacts to the threat.

Finally, Lakeridge Health uses a Cisco Virtual Private Network (VPN) solution to securely connect healthcare partners across the SSHA network. Employees working from home can also gain remote access through a VPN. The VPN capabilities could also be used to extend the network's reach by securely connecting additional healthcare facilities and organizations and giving Lakeridge Health access to new and innovative resources.

According to Deloitte, the key to the solution was its multi-tiered approach. The solution also reflects Cisco's strategy regarding best practices for security as outlined in the Cisco SAFE Blueprint. "We implemented layering so we have a dual set of redundant firewalls, anti-virus protection and intrusion detection," explains Anthofer.

Results

This integrated security strategy has dramatically improved data integrity and confidentiality, while delivering a range of related benefits.

"Cisco provided the tools to proactively manage security on a network level. Now Lakeridge Health has the capability to proactively detect, and respond to, security-related incidents," says Bronson. "In healthcare, the impact of network security goes beyond lost productivity and cost savings. If clinicians lose access to patient care systems the result can be life threatening."

The technology has also eased network management issues. "The system can actually page us if there are security concerns," says Anthofer, adding that it also creates a detailed log for review of any issues that occur.

This comprehensive solution is not only fortifying Lakeridge Health's security capabilities, it's providing a dynamic network foundation for adding advanced new applications and capabilities.

Remote access gives more employees the option of working from home, which Bronson points out, can be a particular advantage during a health crisis such as the SARS outbreak. Remote access also gives Lakeridge Health partners clear cost advantages. "With this VPN and secure [SAFE] architecture we can have a more mobile, flexible workforce," points out Loisel. "In the long run it's significantly more productive and cost-effective."

"With our upgraded network security our staff, partners and patients can feel confident that communications and data are highly protected from outside intrusion or malicious events," says Anthofer. "Our secure connections to our own network, and now to the province-wide Smart Systems for Health network, are allowing us to tap into new resources and cost-effectively improve and expand our services to our growing patient population."



DOES YOUR LAWYER EVEN KNOW WHAT A "PACS" IS?

From IT procurement and outsourcing to intellectual property and privacy issues, the BLG Information Technology Law practice has a seasoned team of professionals dedicated to the provision of pragmatic, practical legal advice specific to the health sector.

We ensure that your technology arrangements reflect the business deal you have struck and that you, the client, fully understand the legal risks that flow from it. Just ask our clients. For more information, please contact us.

Calgary
Michael Whitt
403.232.9571

Montréal
Patrice Martin
514.954.2546

Ottawa
Bernadette Eischen
613.787.3721

Toronto
National Coordinator
Mark Fecenko
416.367.6711

Vancouver
Andrew Loh
604.640.4069



BORDEN
LADNER
GERVAIS

**IT BEGINS
WITH
SERVICE**

Borden Ladner Gervais LLP - Lawyers - Patent & Trade-mark Agents - Avocats - Agents de brevets et de marques de commerce
Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.

www.blgcanada.com