
# Grand River Hospital: The Power of INFRAM for Proving Technology ROI

## How the HIMSS tool helped a Canadian hospital demonstrate the value of investing in cybersecurity

An axiom among cybersecurity professionals says that one of the best ways to demonstrate success is for nothing to happen. By "nothing," they mean that there are no security breaches. No employees or contractors fall for phishing scams. No malware infects network-connected devices and causes systemwide outages.

However, Shival Seth, the Chief Technology Officer (CTO) for Grand River Hospital and St. Mary's Hospital, both in Kitchener, Ontario, wanted to show the hospitals' executives that something *had* indeed happened: Its cybersecurity program had met or beaten industry benchmarks. Leadership had endorsed additional cybersecurity resources, and now it was time to show that those investments were working.

"Security is one of the pieces that, in my opinion, is always being overlooked," Seth said. "Now that we are transitioning to a digital platform – where we have all-electronic health records and our hospital information systems are IT-based – it's extremely important for us to maintain a high level of security, given the rise in ransomware and other cyberattacks that we've seen."

### The rise of ransomware

Ransomware is indeed on the rise at healthcare organizations. A recent study in the *Journal of The American Medical Association* showed that successful ransomware attacks against U.S. hospitals doubled annually between 2016 and 2021, with half of those attacks disrupting care delivery.[1]

Specific statistics on ransomware attacks targeting Canadian healthcare providers are not readily available. However, Canadian providers have announced cyberattacks that led to computer systems disruptions, appointment and procedure cancellations, and/or patient data theft. For instance, two hospitals in Quebec in early 2021 suffered patient care disruptions due to ransomware. Shortly after those attacks, LifeLabs announced it had suffered

***Challenges like these are driving healthcare organizations to find a framework that can help them understand the foundational requirements prior to enabling new technologies."***

**BROOKE LAGGNER** | Healthcare Solution Architect | Cisco

a cyberattack that resulted in the theft of personal data, including lab results and medical histories, for 15 million customers.

These and other cyberattacks factored into Grand River's decision to add more tools to its cybersecurity arsenal in the last few years, especially as the pandemic continued. Because Grand River and St. Mary's are publicly funded, it was important to showcase the considerable investments they had made to protect everything from mobile health applications to electronic health records.

By then, the leaders of Grand River and St. Mary's hospitals had significantly invested in upgrading their cybersecurity programs to better monitor all network traffic and the many devices connected to it. Those investments included solutions pertaining to data detection and inspection, as well as to endpoint detection and response.

## Turning to INFRAM to assess cybersecurity readiness

Seth already had a business relationship with Cisco Systems' Ontario healthcare team and asked them to conduct an independent assessment. The chosen framework was HIMSS' Infrastructure Adoption Model, better known as INFRAM, with a focus on the security domain. INFRAM helps healthcare leaders determine their IT infrastructure's maturity level in terms of digital transformation.

The Cisco team measured the hospitals' perceived cybersecurity readiness by correlating infrastructure maturity to risk and cybersecurity readiness, specifically regarding business resiliency, threat intelligence and ransomware readiness. They focused on the INFRAM subdomains that most impact ransomware prevention and mitigation: endpoint security, threat detection and response, endpoint posture validation and content filtering.

The entire process involved six people – three from Cisco and three from Grand River and St. Mary's – and took about six weeks to go through a checklist with more than 150 questions. To add validity to the framework, the team mapped the hospitals' cybersecurity capabilities and corresponding maturity levels within INFRAM using the NIST Cybersecurity Framework.

"All technologies across cybersecurity scored high once we'd completed the INFRAM assessment," said Brooke Laggner, the Cisco healthcare solution architect who led the project.

Seth preferred not to publicize the hospitals' specific scores but agreed with Laggner: The results were very good and, as intended, impressed the key stakeholders who had originally approved those cybersecurity improvements.

Laggner believes that demand for independent INFRAM evaluations is growing as digital transformations accelerate due to the pandemic and the rise of consumerism in healthcare. While it's possible to conduct self-assessments using INFRAM, a third party provides outside validation and is less likely to misunderstand or misinterpret a question that impacts results.

According to Laggner, there has been an uptick in third-party INFRAM assessments since the early days of COVID-19 lockdowns and the subsequent gradual reopening, forcing healthcare organizations to fast-track digital transformations and to boost network resources that would support both remote workers and patients.

"Since the pandemic started, there's this notion of consumerization of healthcare and the need to directly support patients' care needs at home or at a clinic, beyond an acute-care or post-acute care setting," he said. "Healthcare organizations need to understand what their infrastructure requirements are to be able to interface with patients on those multiple channels. INFRAM is great for that."

Laggner also said that INFRAM can assist with challenges arising from severe workforce shortages as more organizations seek to augment clinical staff and routine tasks with technologies that can improve productivity and reduce friction between providers and patients. These digital health tools require a robust infrastructure that's resilient, flexible, agile – and secure.

***"[INFRAM assessment is] not just doing it once and then forgetting about it. It's a continuous practice to ensure that whatever we are doing is the right approach and that it's the way the industry is going."***

**SHIVAL SETH** | Chief Technology Officer | Grand River Hospital and St. Mary's Hospital

"Challenges like these are driving healthcare organizations to find a framework that can help them understand the foundational requirements prior to enabling new technologies," he said.

## Using assessments to continuously improve

Both Laggner and Seth said any assessment is a discovery process that measures capabilities at a given moment of time. Both agree that continuous evaluation and improvement are key to optimal digital maturation.

"[INFRAM assessment is] not just doing it once and then forgetting about it," Seth explained. "It's a continuous practice to ensure that whatever we are doing is the right approach and that it's the way the industry is going." To know where to go, you must first have a realistic view of where you are.

Said Laggner: "Definitely, having some type of plan that includes a framework such as INFRAM to guide that evidence-based strategy is important. You really must know your current state and aspirational state as well. INFRAM helps with your current state, but you need to decide where to go next."

For Grand River, that's a three- to five-year roadmap as both it and St. Mary's continue to enhance their IT infrastructure and provide more digital offerings to both patients and providers. Maintaining a high level of confidence in their cybersecurity capabilities is important in fulfilling that strategic vision, and that's one reason Seth intends to conduct another INFRAM assessment in two years.

As a CTO, Seth is aware – as all cybersecurity professionals are – of another industry saying about how security is a numbers game. You can stop multiple attacks by malicious actors every day, but all it takes is one successful attempt to do enormous damage.

---

**To learn more about INFRAM, click here or take a look at the Cisco Healthcare portfolio explorer to see how Cisco can help you today.**


**References**

1. Neprash, H.T., McGlave, C.C., Cross, D.A., et al. 2022. Trends in ransomware attacks on US hospitals, clinics and other healthcare delivery organizations, 2016-2021. *JAMA Health Forum* 2022;3(12): e224873. doi: 10.1001/jamahealthforum.2022.4873.