

Pulse Check

The State of Cybersecurity in Canadian Healthcare



Contents & Contributors



Matt Harrison Clough

Freelance Illustrator and the artist behind our cover.



Elias Diab

VP, Cybersecurity Advisory Services, Accerta and author of *Cybersecurity: The New Health Care Emergency in Canada*.



Dr. Benoit Desjardins

Academic radiologist and author of *Pixels under Siege: Cyber Threats to Medical Imaging*.

Navigation Tips

Select contributor head shots to view their articles and sponsor logos to visit their websites

Yellow underlined text indicates a link outside or within the report.



Serge Charette

Director of Solution Engineering, Tanium and author of *Securing the Front Lines of Care: Why Cyber Resilience Is Essential to Modern Healthcare in Canada*.



Ashif Samnani

Cyber Security Principal at MOBIA Technology Innovations and author of *The Great Divide: How Canada's Healthcare Cybersecurity Laws Fall Behind in a Digital World*.



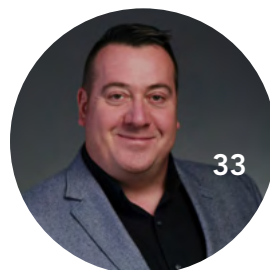
Enza Alexander

Executive Vice-President at ISA Cybersecurity and author of *Five Healthcare Cybersecurity Trends to Watch in 2026*.



André Allen

Director Cyber and Technology Engagement & CISO at INQ Consulting & INQ Law and author of *Cybersecurity and Privacy in Canadian Healthcare: Navigating Critical Challenges in the Digital Age*.



Terry Cutler

CEO of Cyology Labs and author of *A Field Guide for Short-Staffed Teams: Securing Healthcare in a Digital Age*.



François Guay

Founder of the Canadian Cybersecurity Network and author of *Why Every Healthcare Worker Is Now on the Cybersecurity Frontline*.



Charlie Tsao

Engagement and Community Specialist and editor of *Pulse Check*.



Jen Spinner

Creative director of *Pulse Check*.



Securing the Front Lines of Care: Why Cyber Resilience Is Essential to Modern Healthcare in Canada

by [Serge Charette](#), Presented by Tanium

When a hospital's digital infrastructure goes dark, it is not just an inconvenience—it's a crisis. In 2024, one of Canada's largest health networks was crippled by ransomware: surgeries were canceled, patient data was exposed, and care teams were forced back to paper. For patients waiting for a diagnosis or a life-saving procedure, the failure of technology was a direct threat to health.

That incident is far from isolated. In June 2025, Ontario's Information and Privacy Commissioner confirmed that a ransomware attack on a shared hospital IT provider had exposed the personal health information of hundreds of thousands of patients across five institutions. The attack demonstrated the reality of modern healthcare: a breach isn't simply an IT problem, it is a disruption of care.

This is the new reality. Cybersecurity is no longer a back-office concern, it is a frontline issue with direct implications for patient safety. Every unpatched endpoint, every misconfigured cloud setting, and every overlooked medical device is more than just a technical liability, it is a potential break in the chain of care.

The Expanding Risk Landscape

Healthcare IT leaders today face a perfect storm: constant cyber threats that disrupt care, high-stakes compliance demands, tight budget constraints, fragile legacy systems, increasingly complex distributed workforces, and aging operating systems.

At the same time, these systems sit at the intersection of two accelerating forces: the digitization of care and the escalating sophistication of cyber threats. Canada's governments are investing in electronic health records (EHRs), virtual care platforms, and integrated systems to make services more seamless and accessible. Yet every advance in connectivity creates new entry points for attackers.

The Canadian Centre for Cyber Security (CCCS) warns ransomware is no longer a question of if, but when. Its *National Cyber Threat Assessment* underscores how essential services—from hospitals and schools to municipalities—are already being disrupted. “The threat is real, the threat is growing, and we can’t talk enough about it,” as previously stated by Sami Khoury, Head of the CCCS.

94%
of enterprises
discover endpoints
they didn't know
existed.

The numbers tell the same story. A 2025 global analysis of more than 2.25 million Internet-of-Medical-Things (IoMT) devices and 647,000 OT devices across 351 hospitals and healthcare delivery organizations. The study found that 89% of organizations had the top 1% riskiest IoMT devices on their networks—devices with known exploited vulnerabilities (KEVs) and insecure internet connectivity—illustrating how pervasive high-risk exposures are in healthcare environments. In Nova Scotia alone, the Auditor General reported the provincial digital health network comprises over 45,000 connected assets. Inventories and vulnerability management remain incomplete, underscoring exposure at system scale.

This isn't unique to Nova Scotia. A Vanson Bourne study found that 94% of enterprises discover endpoints they didn't know existed; in some environments, scans reveal that as many as one in five devices are unmanaged. This level of blind spot is untenable in healthcare, where every connected device represents both a patient touchpoint and a potential vulnerability.

These weaknesses are compounded by speed. Globally, well over 2,500 new vulnerabilities are disclosed each month. Traditional patching cycles, which often run for weeks or months, cannot keep pace. On average, attackers can exploit these vulnerabilities within five days of discovery, and sometimes on the very same day. Increasingly, they use AI to accelerate this effort, craft convincing phishing lures, and automate intrusions, leaving manual defenders behind.

Adding to the pressure is a chronic shortage of talent. Canada produces fewer than 4,000 cybersecurity graduates annually, while overall demand (including healthcare) is projected at 25,000. Without skilled professionals embedded in our healthcare systems, organizations are left underprepared to face industrial-scale cyberattacks. This shortfall is not just an economic gap, it is a resilience issue.

Defense isn't Enough: Why Resilience Demands AI

Faced with this landscape, healthcare leaders must rethink their approach. For too long, cybersecurity has been defined by defense: building higher firewalls, layering on tools, and trying to keep every intruder out. While this approach remains necessary, it is no longer sufficient. Adding complexity increases costs and lowers efficiency.

Resilience must become the guiding principle. It accepts that compromise is inevitable but ensures systems, and the care they support, continue uninterrupted. In healthcare, that distinction is critical. An outage in retail may inconvenience customers; an outage in healthcare risks delayed diagnoses, canceled surgeries, and diverted ambulances.

This approach starts with visibility, a unified, continuous, real-time inventory of every device, from advanced diagnostic tools in urban hospitals to aging workstations in rural clinics. Yet many healthcare organizations operate with incomplete awareness: legacy systems, unmanaged IoT devices, and siloed data creates blind spots attackers can exploit. In a world of constantly evolving threats, the next generation of visibility is powered by lightweight endpoint agents paired with AI-driven analytics.

Acting as constant sentinels, these agents stream telemetry in real time and can trigger automated, policy-governed

actions, complementing human oversight with immediate response capabilities. When combined with AI analytics, the system moves beyond monitoring to assist decision-making: detecting anomalies, prioritizing risks by criticality and exploit likelihood, and recommending precise next steps, or even auto-remediating within defined guardrails. Together, they shift the balance of speed and precision back in favour of defenders.

Intelligent automation is the next step. With attackers moving faster than ever, manual remediation is too slow. Automated patching, anomaly detection, and compliance enforcement shrink the window of vulnerability and keep critical systems online. AI helps rank issues using live threat intelligence such as KEV and exploit probability signals, focusing effort where it matters most. Rather than predicting the future, these models surface likely hotspots and emerging patterns, so teams can act earlier, with auditability, approvals, and change control intact.

Finally, resilience requires governance. Cybersecurity cannot be confined to IT teams. CIOs, CISOs, compliance leaders, and clinical operations must align on a shared operational picture. Procurement decisions, funding models, and digital health rollouts must all embed security requirements.

This responsibility also extends beyond IT to medical devices, with Health Canada's [updated](#) guidance requiring manufacturers to consider cybersecurity throughout their operational life. Pacemakers, infusion pumps, imaging equipment, all must be secured with the same vigilance as hospital servers. These devices are no longer just clinical tools; they are endpoints in the digital health ecosystem.

Secure by Design Embedded in Digital Transformation

Canada's health systems are modernizing rapidly. British Columbia is upgrading EHRs, while other provinces scale virtual care and remote monitoring. Federally, Bill C-72, the *Connected Care for Canadians Act*, [aims](#) to give Canadians secure, interoperable access to their health data across jurisdictions. Québec has gone even further with Law 5 (*Act respecting health and social services information*), which came into effect in July 2024, setting comprehensive standards for how health data is governed, consented, and secured—establishing a new benchmark for patient control and public trust.

But modernization without embedded security is a false promise. New EHRs, virtual care platforms, and connected systems must be secured by design through funding

requirements, procurement standards, and interoperability rules from day one. This is particularly critical as AI becomes embedded in healthcare innovation. AI-powered diagnostics, predictive patient monitoring, and advanced analytics can improve care but are only as strong as the data and infrastructure behind them. Without robust security, AI can amplify vulnerabilities, creating fragile points in the very systems meant to improve patient care.

Organizations and their leaders, including health systems, should **prepare now** rather than wait.

Ottawa is signaling heightened expectations as the revived *Critical Cyber Systems Protection Act* (Bill C-8) [imposes](#) mandatory cybersecurity programs and incident-reporting on critical infrastructure sectors like banking, energy, and transportation. While healthcare has not yet been formally designated, the law's swift reintroduction makes clear that compliance requirements are expanding; organizations and their leaders, including health systems, should prepare now rather than wait.

Balancing the Scales: Investing in People and Trust

Technology can only carry healthcare so far; resilience also depends on people. Every clinician, administrator, and IT staff member plays a role in protecting systems and patient data. Cybersecurity training should become as routine as infection control protocols or clinical safety drills.

Yet healthcare faces a dual shortage: clinicians and cybersecurity professionals. Hospitals will not be able to hire their way out of this gap. They must instead invest in continuous training for existing staff and plan for tomorrow's demanding workforce needs, supported by automation

that reduces manual workload and allows people to focus on patient care.

At this scale, AI and autonomous tools are essential to help bridge the gap. Emerging copilot tools and AI assistants already guide analysts through investigations, flag anomalies for deeper review, and automate repeatable tasks. In a sector where skilled professionals are scarce, these technologies act as force multipliers, augmenting human judgment

The mandate is unambiguous: Embed resilience into every decision about digital transformation.

rather than replacing it until the workforce can scale to meet the demand. In the long term, incentivized education and training programs must also expand their focus on cybersecurity and AI fluency, ensuring the next generation of healthcare IT professionals is equipped to thrive alongside these advancing tools.

Patients, too, are stakeholders in resilience. Trust in healthcare institutions depends as much on the protection of personal data as it does on the quality of care. A single breach undermines public confidence not just in the affected hospital but in the system as a whole.

The Way Forward: A Digital Health Strategy the Embeds Cyber

Canada's digital health transformation holds immense promise. Connected care can reduce inequities, expand access to underserved communities, and generate insights that improve outcomes nationwide.

When cybersecurity is embedded at the heart of what we do, healthcare organizations can confidently adopt AI-driven diagnostics, remote patient monitoring, and advanced analytics without introducing unmanaged risk. Healthcare modernization is at a critical moment for standardization, and digital transformation provides the opportunity to replace fragmented tools and legacy systems with unified, secure platforms that can scale.

Most importantly, modernization without resilience will not last. The imperative is clear, cybersecurity must be recognized as patient safety. Resilience must be built into every layer of the health system by design: in policy, in procurement, in operations, and in culture. Investments must span technology, workforce readiness, and governance.

For healthcare leaders, the mandate is unambiguous: embed resilience into every decision about digital transformation. This also means securing data before deploying AI in diagnostics, embedding agents on every endpoint to provide real-time visibility, and ensuring automation serves as a shield rather than a liability.

Patients deserve care that is safe, compassionate, and uninterrupted. Anything less is unacceptable.🔒

See [end notes](#) for this article's references.

As Director of Solutions Engineering at Tanium, [Serge Charette](#) leads technical strategy and client engagement for some of Canada's most security-conscious, high-stakes organizations.

Every day, Serge collaborates closely with federal departments, Crown corporations and commercial enterprises to bolster their cyber resilience, enhance endpoint visibility, and expedite threat response—ensuring all solutions are aligned with business goals and regulatory requirements.

With more than two decades of leadership across cybersecurity, enterprise IT, telecommunications, satellite systems, and cloud technologies, Serge brings an extensive senior-level perspective to his current role. As a result, he has earned a reputation as a trusted advisor to senior IT and business leaders, especially in highly regulated environments where public policy, national infrastructure, and innovation converge.

A frequent speaker on topics spanning from cybersecurity agility and endpoint strategy to automation, AI, and platform consolidation, Serge has delivered key sessions at national forums including the Public Sector Network's Government Cybersecurity Showcase and the Canada IT & Security Leaders Forum.

Serge holds a degree in Computer Science and Business Administration and is fluently bilingual in both English and French.



Stay ahead of emerging threats from critical vulnerabilities

Harness complete endpoint visibility that leads to
a reduced attack surface and fewer exploit points.

tanium.com/solutions/healthcare



Canadian Healthcare

