THE HILL TIMES

THIRTY-SIXTH YEAR CANADA'S POLITICS AND GOVERNMENT NEWSPAPER NOVEMBER 4, 2024 $5.00

Opinion

Canada faces a cybersecurity crisis with critical infrastructure at risk

From energy grids to health-care systems, our nation's most essential assets are being targeted by an ever-evolving array of sophisticated threats from both state and non-state actors.

BY JEFF LE

Innovation Minister François-Philippe Champagne said last week that Canada's telecommunications systems face 'nefarious actions by hostile foreign states who seek to compromise our critical infrastructure.' *The Hill Times photograph by Andrew Meade*

Last year, Canadian businesses collectively shelled out a staggering $1.2-billion to recover from cybersecurity incidents. Statistics Canada's latest report—released in conjunction with Cyber Security Month in October—reveals that large enterprises accounted for half of this total, while small and medium-sized businesses each spent $300-million. Alarmingly, StatsCan noted that while fewer businesses are falling victim to attacks, the financial fallout from these incidents is becoming increasingly severe.

Jeff Le is vice-president of global government affairs and public policy at Security Scorecard. *Photograph courtesy of Security Scorecard*

But the crisis extends beyond the private sector. Canada's critical infrastructure is under unprecedented attack. From energy grids to health-care systems, our nation's most essential assets are being targeted by an ever-evolving array of sophisticated threats from both state and non-state actors.

The high-profile ransomware attack on the city of Hamilton, Ont., which paid over $5.7-million to recover from the extensive damage, is just one example. A ransomware attack at five southwestern Ontario hospitals forced critical systems offline for weeks, costing those organizations upwards of $7.5-million. And, a warning released in May 2024 that pro-Russia hacktivists are targeting North American critical infrastructure and pose serious physical threats to insecure operational technology at these organizations shows the proliferation of these types of risks.

As Innovation Minister François-Philippe Champagne noted in his appearance at the Senate National Security, Defence, and Veterans Affairs Committee on Oct. 28, "Canadians increasingly rely on the internet and wireless services in their day-to-day lives. Anyone who has kids or who operates a business in this country will know this to be true, from financial transactions and e-commerce, to education, health care and emergency services, such as 9-1-1. These critical services need to rely on a robust, modern and safe telecommunications system. We know, however, that risks to this critical infrastructure are on the rise," he said.

Champagne continued: "We need to be vigilant and engage when we talk about cyber threats and cybersecurity and with eyes wide open. The risks I am talking about include nefarious actions by hostile foreign states who seek to compromise

our critical infrastructure … and telecom products from global suppliers that pose an unacceptable risk to the Canadian telecommunications systems."

This is a wake-up call: we cannot afford to be complacent in the face of such relentless aggression. Safeguarding Canada's infrastructure isn't just a province, territory, or national imperative. It has far-reaching global implications. Disruptions to energy, transportation, and healthcare systems can trigger a domino effect, impacting global supply chains, economic stability, and international security.

As Canada navigates the increasingly complex terrain of cyber threats, the introduction of Bill C-26, which amends the Telecommunications Act and enacts the Critical Cyber Systems Protection Act, marks a significant legislative step toward safeguarding our critical infrastructure. However, this bill is just the starting line. Operationalizing it effectively is paramount. As we move forward, it's crucial to recognize that legislation alone cannot shield us from the evolving threats posed by cybercriminals and state-sponsored attacks.

It's time for a paradigm shift in how organizations approach cybersecurity, one that embraces standardized risk measurement and management across the entire supply chain as the foundation for a resilient defence strategy.

Why real-time cyber resilience matters

Cyber resilience is dynamic and constantly evolving. Today's cyber-threat actors are more skilled and adaptive, using advanced techniques for targeted attacks. As a result, decision-makers in both public and private sectors must prioritize real-time assessments of their cybersecurity posture. It's not just about being secure today, but also having the capability to quickly detect, respond to, and recover from future incidents.

Organizations need more than periodic system check-ups; they require real-time risk metrics that provide actionable insights and support a proactive defence. Under Bill C-26, identifying and mitigating cybersecurity risks associated with supply chains and third-party services is essential. Continuous monitoring is crucial not only for threat detection, but also for swift mitigation, helping groups address security gaps before significant harm occurs.

Senators currently studying Bill C-26 at the National Security Committee must consider establishing mechanisms to measure the bill's effectiveness. By defining and tracking clear metrics, we can significantly bolster cyber resilience and restore confidence in digital infrastructure.

Fostering a resilient cybersecurity culture

As a key member of the Five Eyes alliance, Canada plays a vital role in global cybersecurity efforts, setting a benchmark for allied nations. Protecting our people at home and abroad requires an integrated approach to cyber capabilities. Recent collaboration among provincial chief information security officers at the Canadian Centre for Cyber Security highlights the importance of a co-ordinated defence, as cyber threats know no borders.

Public awareness and digital literacy are also essential for empowering Canadians to recognize and mitigate cyber risks. Our nation faces significant challenges in safeguarding its citizens and critical infrastructure, necessitating a long-term strategy that anticipates future threats. Let's commit to building a more secure cyber landscape together, ensuring that as we advance technologically, we do not leave our defenses behind. The time for action is now.

Jeff Le is vice-president of global government affairs and public policy at Security Scorecard, the global leader in cybersecurity ratings and the pioneer of supply chain detection and response solutions.

The Hill Times