Cybersecurity: The Downside of Digital Interconnectivity

As 2025 begins to unfold, Canada will continue to be affected by the frequency and increased sophistication of cybersecurity threats. While new technology and developments in AI and quantum computing have led to increased efficiency and communication, they have also made the digital landscape more complex to navigate.

The financial impact of data breaches is substantial. In 2024, Canadian organizations faced an average cost of CA$6.32 million per data breach. The financial services sector experienced even higher costs, averaging CA$9.28 million per breach.

The Bank of Canada highlights that the financial sector was an attractive target for malicious cyber operators during the pandemic, with new threats linked to evolving central banking activities such as updated payment systems and digital currencies. To combat the increased threat, a clear strategic vision is needed to strengthen the resilience of the Canadian financial sector.

To defend against these threats, cybersecurity leaders need to be stay on top of current trends and adopt forward-thinking, proactive measures.

Here are 6 cybersecurity trends affecting the Canadian finance industry:

Increasing Sophistication of Cyber Threats

Cyberattacks targeting the financial sector are becoming more frequent, sophisticated and damaging. In 2024, phishing attacks were the most common type of initial attack

vector representing 14% of incidents. Some threats such as Chameleon, a device-takeover Trojan discovered in 2022, use a technique masquerading as a CRM app. The continuing evolution of trends in the digital race highlights the increasing need for robust cybersecurity measures.

Rise in Ransomware Attacks

Ransomware remains a significant threat to Canada's critical infrastructure, including the financial sector. The National Cyber Threat Assessment 2025-2026 identifies ransomware as the top cybercrime threat, directly disrupting critical infrastructure entities. Since 2020, ransomware attacks have increased in scope, frequency and complexity. They will continue to be the most impactful cyber threat facing Canadian organizations in the next two years as criminals constantly refine their tactics to maximize profits.

Integration of Artificial Intelligence (AI) in Cybersecurity

The adoption of AI in cybersecurity is on the rise. One of the seismic shifts in the world of cybersecurity is due to the rise in AI-powered threats. Cybercriminals are using AI to enhance the quality, scale and precision of malicious cyber threat activity. They are using generative and predictive AI tools such as LLM's (large language models) to support their work processes. AI technology is also increasing the quality and scale of foreign influence campaigns using fictitious social media accounts and online personas to amplify engagement.

While AI can be used by cybercriminals, it's also being used as a defense mechanism to avoid them in the first place. Organizations need to establish responsible AI governance to minimize security and privacy risks.

Increased Regulatory Focus on Cybersecurity

Regulatory bodies are increasingly focusing on cybersecurity risks. The Office of the Superintendent of Financial Institutions (OSFI) has identified AI and cybercrime as top risks to Canadian banks, highlighting the need for more robust cybersecurity measures.

Bill C-26 contains amendments to the *Telecommunications Act* that would give the federal government legal authority to ban Canadian telecommunications service providers (TSP's) from using certain suppliers deemed to be "high risk." This would mark a significant shift in Canada's cybersecurity landscape introducing new powers and placing the onus on organizations to prepare for compliance.

Increase in Cybersecurity Investments

Despite overall reductions in IT budgets, Canadian companies are allocating a larger portion to cybersecurity. This year-over-year trend underscores the prioritization of cybersecurity budgets to mitigate potential negative impacts on business operations.

As cyber threats become more sophisticated, the Government of Canada has made cybersecurity a priority. The 2024 budget proposed $917.4 million over five years to enhance intelligence and cyber operations programs to respond to these evolving threats.

Focus on the Human Element

The rise in cybersecurity threats highlights the need for public awareness and education to mitigate these threats. Young people in particular are living in a perpetually interconnected world and need to be made aware of the potential risks early on. Moving forward, education will be key for companies as well as they seek to navigate themselves in the ever changing digital landscape.

To combat the rising threat from more frequent and sophisticated cyberattacks, cybersecurity leaders must embrace forward-thinking and proactive measures. Diversified training programs need to be implemented to enhance employee awareness of AI driven threats. Moving forward, gaining a thorough understanding of cybersecurity trends will be the best weapon for safeguarding data and ensuring resilience against such a damaging and relentless enemy.