Securing Canada's Digital Future

A Collaborative Approach to National Cyber Resilience

ANCHORAM CONSULTING

2025-06-30

anchoramconsulting.ca

Executive Summary

This whitepaper summarizes the insights gathered from Anchoram's roundtable titled 'Future of Cyber in Canada.' The event, held during Toronto Tech Week (June 23–27, 2025), brought together cybersecurity and technology leaders from the public and private sectors to share their concerns, ideas, and proposals for improving Canada's national cybersecurity posture.

In today's increasingly digitized world, the amount of data accessed, utilized and shared continues to grow across a growing number of connected devices. The dark side of this robust growth in connectivity is the pronounced increase in cyber vulnerabilities and privacy violations. In the case of individuals, this digitized connectivity removes transactional friction and allows for a multitude of conveniences. In the case of businesses and institutions, it is used to drive efficiency, reduce costs and build data-driven businesses that are better suited for the future. The overall threat surface is growing exponentially as digital adoption accelerates rapidly, which makes individuals and businesses more and more vulnerable.

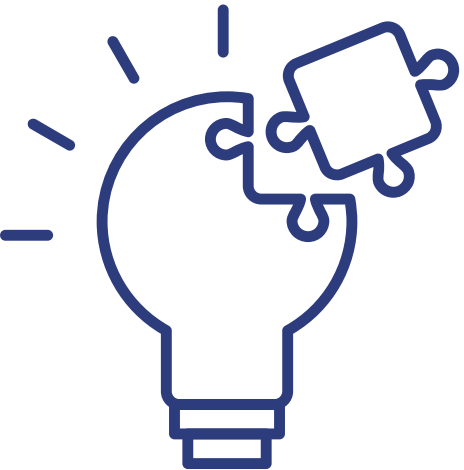
The shifting global geopolitical landscape has profoundly impacted Canada's cyber threat environment, transforming it into a more complex and volatile space. Canadian public and private sector organizations continue to deal with on a daily basis, sophisticated and frequent cyber threats. From ransomware to social engineering and supply chain breaches, the scale of attacks has escalated, impacting both public and private sectors. Despite significant improvements in awareness and spending, gaps persist in legislation, cyber-literacy, insurance, and public-private coordination.

Anchoram's roundtable titled 'Future of Cyber in Canada' was attended by cybersecurity and technology leaders from the public and private sectors to discuss Canada's national cybersecurity posture. Discussion topics included government and private sector responsibilities, the impact of legislation, the growing threat of ransomware, the need for sovereign cloud infrastructure, quantum safety, and the urgency of cyber education. The paper concludes with actionable recommendations aimed at supporting federal cyber policy initiatives.

ANCHORAM CONSULTING

Problem Statement

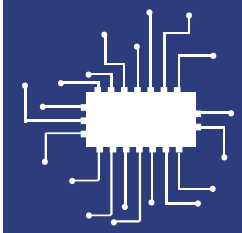
Despite years of incremental improvements in cybersecurity across sectors, Canada remains highly vulnerable to cyber attacks. Many organizations – especially municipalities and small-to-mid-sized enterprises – lack the funding, education, and coordinated support needed to implement resilient cybersecurity programs. Meanwhile, cyber threats continue to escalate in complexity, frequency, and cost. The absence of enforceable standards and inconsistent collaboration between levels of government have led to fragmentation in cyber defense. The limited impact of current legislation, combined with workforce shortages and insufficient user education, leaves critical systems and data at risk.



Primary Challenges

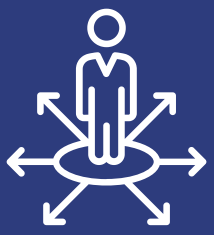
- The human element remains the weakest link, making social engineering a persistent threat vector with widespread incidents caused by human error.
- Significant variability in security maturity exists across regions and sectors. Federal and Provincial / Territorial governments are more mature than municipalities across Canada.
- The existence of cyber regulations varies across the country including limited enforcement and the absence of robust accountability frameworks—unlike in privacy legislation, where models such as J.R.A.D. (Justification, Risk, Accountability, Documentation) offer a clearer structure for governance and compliance. We continue to see risks around human-based vulnerabilities, suggesting we should not looking just at the information type, but the broader risk factors.

Introduction



Cybersecurity is no longer just a technology issue; it is a foundational element of public trust, economic security, and national sovereignty. The roundtable featured voices from public administration, financial services, healthcare, and AI-based technology sectors. The conversations reflected the need for both immediate interventions and long-term strategic investments.

Key Opportunities



Key opportunities are emerging that can significantly bolster Canada's cyber resilience. We're seeing an expansion of cyber awareness across both government and industry, a crucial step in fostering a more secure digital culture. Furthermore, the advent of AI and cloud-native technologies offers scalable security advantages, providing innovative tools to defend against evolving threats. Finally, the growing momentum behind trusted partnerships between the public and private sectors presents a powerful collaborative model for developing and implementing robust cybersecurity strategies.

Bill C-8 and Legislative Readiness

- The potential of Bill C-8 (formerly C-26) to improve breach reporting and critical infrastructure protection.
- Concerns were raised over its delayed progress and lack of agile enforcement mechanisms.
- Several attendees stressed that legislation without behavioral change and executive accountability will fall short.

Federal and Provincial Agency Effectiveness

- The Canadian Centre for Cyber Security (CCCS) is regarded as effective but under-leveraged at the municipal & small medium enterprise levels.
- Privacy commissioners are often drawn into cyber matters, due to the impact on personal information, although not clearly defined as a core responsibility.
- Broader jurisdictional collaboration and more actionable guidance are needed.

Enhancing Education and Awareness

- Cyber literacy must be integrated into school curriculum as early as grade school.
- Education campaigns could mirror successful public health initiatives, such as those used to reduce smoking.
- Awareness programs for executives and staff are essential to drive culture change.

Current State and Strategic Outlook

Cyber Resilience and Risk Accountability

- Attendees advocated for executive performance to be tied to measurable cyber readiness KPIs.
- Boards must treat cybersecurity with the same priority as financial and safety metrics.
- Public and private sector corporations need real-time dashboards to monitor vulnerabilities, breaches, and compliance status.

Sovereign Cloud and Infrastructure Resilience

- Participants discussed Canadian sovereign clouds versus partnering with hyperscalers, recognizing ongoing hyperscalers investments.
- Sovereignty concerns are rising amid increasing geopolitical instability and data residency laws.
- Importance of helping less mature organizations know where to start in compliance frameworks (similar to Australia's 'Essential Eight').

Ransomware and Continuity Planning

- Repeated targeting of organizations due to inadequate remediation of initial compromises.
- Emphasize on the importance of tabletop exercises, proactive patching, and up-to-date configurations.
- Negotiation with ransomware actors is controversial – advised against it unless critical systems are disrupted.

Current State and Strategic Outlook

ANCHORAM CONSULTING

Workforce and Educational Gaps

- Canada needs to invest in early STEM and cyber education to create a pipeline of domestic talent.
- Attendees cited lack of access to AI/quantum readiness guidance as an urgent barrier.
- There is broad support for expanding post-quantum cryptography research and AI-based threat detection.

Supply Chain and Third-Party Risk

- Multiple breaches discussed during the session were traced to third-party vendors or inherited code.
- Supply chain attacks often occur several layers downstream, making transparency and traceability crucial.
- Lack of standardization provisions and their ineffectiveness across contracts and suppliers was a shared concern.

Strengthening Canada’s Cyber Resilience: A Path Forward

Canada's National Cyber Security Strategy, should be a key point of reference for individuals responsible for cyber security. To safeguard our digital future and bolster resilience against increasingly sophisticated attacks, Anchoram and the attendees, through collaborative discussion, propose the following **five strategic imperatives:**

1. Cultivating a Cyber Aware Nation

Ensure Provinces and Territories have the tools to support local school boards to ensure cybersecurity is integrated into K–12 education. Early education will continue to promote early cyber careers and equip Canadians with essential digital safety knowledge. Additionally, sustained government-led public awareness campaigns, like "Get Cyber Safe," are vital to educate all Canadian residents on cyber threats, online safety best practices, and how to report suspicious activities.

2. Enhancing Government and Critical Infrastructure Security

To ensure accountability and drive continuous improvement, we must mandate real-time cyber dashboards for all government agencies and Crown corporations. These metrics should be about risk and vulnerability, not Red, Green, Yellow - these are outdated indicators. This will provide transparent insights into their security posture and facilitate timely interventions. Furthermore, securing Canada's digital backbone requires strategic investment. We believe that rapid passage of Bill C-8 is required as a key aspect of National Security.

3. Expanding Support and Incentivizing Best Practices

The Canadian Centre for Cyber Security (CCCS) exists to protect all Canadians, leaders in public and private sector corporations need to understand how to leverage the power of the CCCS, much like they have done with other risk management assets. To accelerate the adoption of robust security practices across the private sector, we must incentivize the adoption of recognized compliance frameworks across sectors through various mechanisms, such as grants, tax credits, or preferred procurement status. Cyber awareness and accountability needs to be seen as core to governance boards, councils and agencies, boards and commissions.

4. The Imperative for Cyber Hygiene: A Parallel to Health and Safety

Implement a comprehensive, mandatory national cyber hygiene policy and compliance framework for all Canadian organizations, akin to existing health and safety regulations, to establish a baseline of security practices and foster a nationwide culture of cyber resilience.

5. The Imperative for Cyber Hygiene: A Parallel to Health and Safety

To truly embed cybersecurity into organizational culture, we recommend organizations consider a closer connection between leadership performance reviews and cyber readiness KPIs and breach response maturity. This could be first modelled by all levels of government and related agencies. Finally, recognizing that cyber threats transcend national borders, Canada must establish national and international collaboration to harmonize standards and incident response protocols. By working with our allies and domestic partners, we can create a more unified and effective defense against global cyber threats.

Ongoing review and enhancements to Canada's National Cyber Security Strategy is vital for Canada to navigate the complexities of the modern cyber landscape and safeguard its digital future. Anchoram and its dedicated stakeholders are prepared to partner with federal ministries to implement these solutions, thereby fostering trust and enhancing resilience within Canada's digital ecosystem.

About Anchoram Consulting

The idea for Anchoram Consulting bore out of a group of experienced professionals with extensive experience working for large corporate, government and consulting organisations who shared common vision to found a consulting organisation which genuinely cares for its clients and its people Anchoram Consulting consists of senior and experienced individuals who have worked in public sector, industry and large global consulting powerhouses, who share a common purpose to serve organisations with strong client service ethos.

Anchoram team constitutes of experts in **enterprise risk management**, **cyber and protective security**, **program and project management**, **critical infrastructure security** and **data and information management**.

Our Locations

Toronto

130 King St West, Suite 1900,
Toronto ON, M5X 1E3

Ottawa

Fairmont Chateau Laurier, 1 Rideau Street,
7th and 8th Floors, Ottawa ON, K1N 8S7

Our Leadership Team

Chris Moore

President and CEO - Anchoram Canada

E: Chris.Moore@anchoramconsulting.ca

Glenn Ashe

CEO - Anchoram Global

E: Glenn.Ashe@anchoramconsulting.ca

Harry Cheema

Practice Lead Partner - Cyber Security

E: Harry.Cheema@anchoramconsulting.ca

ANCHORAM CONSULTING

anchoramconsulting.ca