Insights into Bill C-26: A Comprehensive Analysis of Canadian Cybersecurity Policy

A 360 Degree Perspective | August 2024

Bill C-26, titled "An Act Respecting Cyber Security," seeks to amend the Telecommunications Act and introduce the Critical Cyber Systems Protection Act (CCSPA). The legislation aims to enhance the security of Canada's telecommunications systems and critical infrastructure.

Bill C-70, the Countering Foreign Interference Act, has amended the draft Bill C-26 to establish a new Secure Administrative Review Proceedings (SARP) regime under the Canada Evidence Act, replacing the current judicial review process under the Telecommunications Act. This new regime, which will also apply to compliance orders under the CCSPA, introduces special counsel to handle sensitive information during judicial reviews or appeals. These changes address due process concerns raised by critics of Bill C-26.

The authors underscore the significance of this legislation in fortifying Canada's cybersecurity posture and heralding a new era of proactive engagement in safeguarding critical infrastructure.

The Contributors

A team of industry leaders with diverse experiences collaborated to offer this analysis of Bill C-26, shedding light on the Bill's significance and impact, and offering practical guidance for affected organizations.

- Gary Miller, Field Chief Technology Officer at Compugen Inc.
- Bob Gordon, Strategic Advisor at the Canadian Cyber Threat Exchange (CCTX)
- TECHNATION Canada
- Brent Arnold, Partner at Gowlings WLG; Director, The Canadian Internet Society

Table of Contents:

Amendments to the Telecommunications Act

The proposed amendments to the Telecommunications Act grant the government authority to mandate necessary security actions to secure Canada's telecommunications systems. This provides the legal framework for the government to enforce cybersecurity measures across the telecommunications sector.

Introduction of the Critical Cyber Systems Protection Act (CCSPA)

The CCSPA is designed to bolster cyber defenses within critical sectors of the Canadian economy, aiming to safeguard national security and public safety. It mandates cybersecurity programs, third-party risk management, incident reporting, and enforcement measures across federally regulated sectors operating critical cyber systems. These sectors include telecommunications services, interprovincial or international pipeline and powerline systems, nuclear energy systems, transportation systems, banking, and clearing and settlement systems, as specified in Schedule 1 of the Act.

While both aspects of the Bill are highly consequential, this Perspectives Paper will primarily focus on the introduction of the CCSPA and the far-reaching implications of such.

Who Bill C-26 Impacts

Impact on Designated Operators

Bill C-26 affects a broad range of Canadian businesses, particularly those designated by the Government as operators of critical cyber systems. These operators are subject to several new obligations, which are detailed below. Operators will transfer many obligations to their supply chains and third-party suppliers, thus broadening the impacted parties.

Obligations for Designated Operators

1. Establish + Implement a Cybersecurity Program

Operators must develop and implement a comprehensive cybersecurity program within 90 days of designation. This program should include risk mitigation measures and a governance framework to manage organizational risks. It should address the following key areas:

- Identify + Manage Organizational Cybersecurity Risks: This includes risks associated with the operator's supply chain and use of third-party products and services.
- Protect Critical Cyber Systems: Implement measures to prevent unauthorized access or disruptions.

- Detect Cybersecurity Incidents: Develop capabilities to identify potential cybersecurity incidents.
- Minimize the Impact of Incidents: Establish response plans to mitigate the effects of cybersecurity incidents.
- Compliance with Prescribed Measures: Follow any additional measures specified by regulators.

2. Manage Third-Party Risk

Operators must ensure their cybersecurity program includes measures to identify and mitigate risks from their supply chain and third-party services. This includes:

- Conducting risk assessments of third-party products and services.
- Implementing contractual obligations to ensure third-party compliance with cybersecurity standards.
- Monitoring third-party cybersecurity practices and addressing identified risks.

Supply chain and third-party providers can expect to see direct impacts in establishing their cybersecurity programs, reporting, contractual obligations to name a few.

3. Enhance Incident Reporting

In the event of a cybersecurity incident, operators are required to:

- Report the incident to the Communications Security Establishment (CSE) within a period prescribed by the appropriate regulator, not exceeding 72 hours.
- Notify the appropriate regulator immediately following the incident report to CSE.

4. Comply with Binding Cybersecurity Directions

Operators must comply with any binding cybersecurity directions issued by the Governor in Council (federal cabinet) or the appropriate regulator to protect critical cyber systems.

5. Maintain Records in Canada

Operators must maintain detailed records of their cybersecurity programs, supply chain risk management activities, cybersecurity incidents, and compliance with directives. The retention period for these records will be specified by the appropriate regulator.

Regulatory Oversight + Penalties

Regulatory bodies will oversee compliance with Bill C-26. They are empowered to review an organization's cybersecurity program and hold them accountable for their security practices. Penalties for non-compliance include:

- Administrative Monetary Penalties: Up to C$15 million for designated operators and C$1 million for directors and officers.
- Criminal Charges: Non-compliance with certain provisions may lead to fines and imprisonment.
- Expanded Powers for Regulators: Regulators can compel information, conduct inspections, and issue notices of non-compliance.

What Now?

Industry leaders agree that Bill C-26 significantly strengthens Canada's cybersecurity. The legislation addresses critical gaps and aligns with global standards. However, it poses challenges, especially for smaller organizations that may struggle with compliance. Uncertainty about which operators fall under the legislation and the expected standards hampers their ability to prepare. The lack of concrete timelines for compliance further complicates matters. Additionally, penalties for contravening yet-to-be-determined regulations are concerning. The Governor in Council's forthcoming regulations will provide clarity on designated operators. It is hoped that sector-specific regulators will offer detailed guidance on standards and best practices, like successful privacy regulation models.

Collective Insights + Perspectives

1. Advancement in Cybersecurity

Bill C-26 aligns Canada with its global allies, reinforcing national security against persistent and sophisticated cyber threats. It marks a critical step forward in protecting the nation's critical infrastructure. In essence, it is the formalization of what many organizations and sectors have long considered essential best practices.

2. Implementation Challenges

Smaller organizations may face significant challenges in meeting the requirements of Bill C-26 due to limited resources. Regulatory clarity and support will be essential to help these organizations achieve compliance without excessive burden. There must be collaborative initiatives to "lift all boats".

3. Harmonization of Standards

One of the key strengths of Bill C-26 is its aim to harmonize cybersecurity measures across various sectors. This harmonization is expected to streamline governance and enhance the resilience of critical infrastructure. By aligning cybersecurity practices across sectors, Canada can create a more unified and robust defense against cyber threats.

4. Proactive Engagement

Organizations must adopt a risk-based approach to cybersecurity, enhancing their resilience and preparedness for potential cyber incidents. This involves continuous assessment and improvement of cybersecurity practices to stay ahead of emerging threats – for themselves, their sector and their supply chains.

Recommendations for Stakeholders

Three primary stakeholder groups are impacted by the Bill and each should consider proactive actions in anticipation of it becoming legislation.

Regulators:

- Provide Clear Guidelines: Regulators should offer detailed guidance on the specific requirements of a cybersecurity program to ensure organizations understand their obligations.
- Support Smaller Organizations: Develop support mechanisms to help smaller organizations comply with the legislation, such as providing resources, tools, and incentives.
- Harmonize Requirements: Work towards harmonizing cybersecurity standards across sectors, and with current obligations, to reduce complexity and facilitate compliance.

Designated Operators:

- Assess Current Cybersecurity Programs: Evaluate existing cybersecurity practices and identify any gaps that need to be addressed to meet the requirements of Bill C-26.
- Enhance Third-Party Risk Management: Strengthen third-party risk management practices, including contractual obligations and monitoring of third-party cybersecurity measures.
- Prepare for Incident Reporting: Develop and test incident response plans to ensure timely and effective reporting of cybersecurity incidents.

Supply Chain + Third-Party Suppliers:

- Understand Legislative Impact: Recognize how Bill C-26 affects your relationship with designated operators and prepare to meet new cybersecurity expectations.
- Collaborate with Customers: Engage with customers to understand their requirements and ensure your cybersecurity practices align with legislative obligations.
- Enable Independent Reviews: Be prepared for independent reviews of your cybersecurity program as part of the compliance process.

Conclusion

Bill C-26 is a pivotal development in Canada's cybersecurity landscape, aiming to fortify the nation's critical infrastructure against cyber threats. While the legislation introduces significant obligations for designated operators and their supply chains, it also provides a framework for enhancing national security and public safety.

Looking Ahead

As Bill C-26 progresses through the legislative process, stakeholders must prepare for its implementation. This involves understanding the requirements, assessing current cybersecurity programs, and enhancing resilience against cyber threats. Regulatory bodies will play a crucial role in providing guidance and support to facilitate compliance.

Call to Action

Three key stakeholder groups have specific actions to take in preparation for and execution of the obligations under the Act:

1. Appropriate Regulators:

Prescribe with greater certainty the elements of a cybersecurity program, appreciate and reconcile with existing regulatory regimes, and work towards harmonization.

2. Designated Operators:

Seek regulatory clarity, assess current programs, enhance resilience, and improve third-party risk management.

3. Supply Chain and Third-Party Suppliers:

Understand your role, prepare for assessments, and align with customer expectations.

Regardless of the process and timing toward becoming an Act, stakeholders should act immediately to put in effect essential programs, collaborative initiatives, and enhanced sharing and reporting.

Bill C-26 represents a significant milestone in Canada's cybersecurity journey. By fostering collaboration, communication, and proactive engagement, Canada can enhance its cybersecurity resilience and protect critical infrastructure from evolving cyber threats. The collective efforts of regulators, businesses, and industry stakeholders will be essential in realizing the Bill's potential and fortifying Canada's cybersecurity landscape.

Compugen Inc.

As Canada's largest privately-owned and operated Technology Ally, we help organizations realize new possibilities. To innovate industries, transform businesses, connect communities, and drive meaningful change, we must think bigger, reach broader, and act bolder. Through knowledge, curiosity, and collaboration, Compugen helps organizations deliver experience by design. This is what it means to be human-centered and technology-enabled.
Get an ally in your technology journey.

Visit www.compugen.com to start now.

CCTX

The CCTX is Canada's cross-sector, private sector organization providing actionable cyber threat intelligence. Our members include organizations of all sizes, from the largest to smallest. We gather, enrich, analyze, and share cyber threat information. The CCTX's almost 200 members collaborate and share information. Our members improve their cyber posture and resilience and reduce their cost of security by learning from each other, having a trusted group to discuss challenges, and sharing experiences.

To learn more contact us at info@cctx.ca.

TECHNATION Canada

TECHNATION is the industry-government nexus for technology prosperity in Canada. As a member-driven, not-for-profit, TECHNATION unites Canada's technology sector, governments, and communities to enable technology prosperity in Canada. TECHNATION champions technology prosperity by providing advocacy, professional development and networking opportunities across industry and governments at all levels; connecting Canadian scale-ups with global tech leaders; engaging the global supply chain; and filling the technology talent pipeline.

Learn more at www.technationcanada.ca.

Gowling WLG

Gowling WLG is an international law firm comprising the members of Gowling WLG International Limited, an English Company Limited by Guarantee, and their respective affiliates. Each member and affiliate is an autonomous and independent entity. Gowling WLG International Limited promotes, facilitates and co-ordinates the activities of its members but does not itself provide services to clients.

Learn more at www.gowlingwlg.ca.