A report released by the Canadian Senate on Oct. 29, 2018, provocatively titled: Cyber.assault: It should keep you up at night, raises alarm about the state of cyber security in Canada, and calls for the creation of a new federal ministry to fend off cyber attacks.

The report, originally mandated for release in June but extended to the fall, follows a year of hearings with testimony from public and private stakeholders from Public Safety Canada, the Communications Security Establishment and the Canadian Security Intelligence Service to the Bank of Canada, MasterCard and the Canadian Bankers Association.

The Committee begins with facts highlighting the sheer enormity of the problem, summarizing recent privacy breaches affecting Canadians by the tens of thousands and, in some cases, compromising the data of nearly 2 million Canadians and placing the 10 million Canadians compromised by various breaches in the global context of 978 million victims of cyber crime. Witnesses before the Committee noted that "consumers generally have few options for recourse when their personal information is stolen" and noted that the Royal Canadian Mounted Police "may not have the capacity to commence any new investigations into major cyber threats."

The Committee's brief report sets out the prongs of a new strategy to combat this increasing threat, including improving consumer awareness of threats posed by the Internet of Things, assisting businesses and ensuring compliance with privacy laws, and improving Canada's cyber
Recommendation 1:

All levels of government prioritize cyber security education in their cyber security strategies. To achieve this, the federal government should enable and fund:

- Cyber security skills training programs, in collaboration with the provinces, territories and municipalities, to assist businesses with their cyber security needs;
- Three national centres of excellence in cyber security research in order to promote basic research in the science of cyber security at the university level and to encourage Canadians to pursue education and careers in cyber security-related fields, with the goal of doubling the number of graduates with cyber security expertise in the next four years; and
- A national cyber literacy program, led by the Canadian Centre for Cyber Security, to educate consumers and businesses on how to become cyber resilient. The program should promote awareness of the importance of cyber security needs at the junior and senior high school levels and encourage further education in science, technology, engineering and mathematics programs.

Recommendation 2:

The federal government develop standards to protect consumers, businesses and governments from threats related to the Internet of Things devices.

Recommendation 3:

The federal government develop a rapid and responsive national cyber security information sharing framework and make any necessary legislative changes to the Privacy Act and the Personal Information Protection and Electronic Documents Act to allow information sharing about cyber threats within the private sector and between the private sector, government and relevant international organizations.

Recommendation 4:

The federal government identify any deficiencies in information sharing and determine how law enforcement agencies can be provided with the necessary tools to actively and quickly
share information and work with other jurisdictions in the prosecution of cyber criminals.

**Recommendation 5:**

The federal government develop a consistent set of leading cyber security standards that are harmonized with the highest international standards and would apply to all entities participating in critical infrastructure sectors.

**Recommendation 6:**

The federal government provide incentives for all businesses, particularly those in critical infrastructure sectors, to improve their cyber security practices, such as allowing accelerated capital cost allowance deductions to companies under the Income Tax Act for investments in cyber security.

**Recommendation 7:**

The federal government modernize Canada's privacy legislation to take into account emerging cyber security concerns and international standards. It should provide the Office of the Privacy Commissioner with new resources to carry out its mandate and provide the Commissioner the power to make orders and impose fines against companies that have failed to take adequate measures to protect customers' personal information.

**Recommendation 8:**

The federal government create a new federal minister of cyber security. This minister would be responsible for cyber security policy, including the national cyber security strategy, and have oversight over the new Canadian Centre for Cyber Security and the National Cybercrime Coordination Unit.

Until the minister of cyber security is created, the person designated as the federal lead for cyber security should report directly to the Prime Minister on these matters.

Lastly, the Prime Minister should table an annual report to Parliament on issues related to Canada's cyber security strategy.

**Recommendation 9:**
The federal government create a federal expert task force on cyber security to provide recommendations regarding the national cyber security strategy that would establish Canada as a global leader in cyber security.

**Recommendation 10:**

The federal government require its departments and agencies to report privacy breaches to the Office of the Privacy Commissioner.

and

The federal government continue to implement best practices for the federal public service to ensure that properly secured devices are used to protect sensitive information.

[Emphasis added.]

This report lands just a few months after the announcement of a new federal cyber security strategy, and mere weeks after the launch of the new Canadian Centre for Cyber Security (the "CCCS")[6] referenced throughout the report. The CCCS is already pursuing a mandate to improve public education about cyber risk as contemplated in Recommendation 1, and has entered into an agreement with the Canadian Cyber Threat Exchange to facilitate some degree of the public-private sharing of threat information contemplated by Recommendation 3.

It will be interesting to see how quickly and to what extent the report is adopted by the federal government private sector stakeholders.

---


[4] Senate Canada, Report of the Standing Senate Committee on Banking, Trade and Commerce, Cyber.assault: It should keep you up at night (Ottawa: October 29, 2018) at p.11
Senate Canada, Report of the Standing Senate Committee on Banking, Trade and Commerce, Cyber.assault: It should keep you up at night (Ottawa: October 29, 2018) at pp.6-10 online:
https://sencanada.ca/content/sen/committee/421/BANC/Reports/BANC_Report_FINAL_e.pdf.

For more on these developments, see Brent J. Arnold, "Canada Hits 'Refresh' on Cyber in 2018 with the Canadian Centre for Cyber Security" (October 11, 2018) online:

NOT LEGAL ADVICE. Information made available on this website in any form is for information purposes only. It is not, and should not be taken as, legal advice. You should not rely on, or take or fail to take any action based upon this information. Never disregard professional legal advice or delay in seeking legal advice because of something you have read on this website. Gowling WLG professionals will be pleased to discuss resolutions to specific legal concerns you may have.

Related  Tech

Author

Brent J. Arnold
Partner - Toronto

Email
brent.arnold@gowlingwlg.com

Phone
+1 416-369-4662

vCard
Brent J. Arnold