CGI

Experience the commitment®

Will Canada's Cybersecurity Legislation Impact Your Business?

Be aware of your obligations

In 2015, the Government of Canada introduced a number of legislative amendments and programs in an effort to keep pace with the digital economy and growing cyberthreats to Canadian businesses and citizens. These initiatives, meant to strengthen our collective cyberresiliency, require Canadian businesses of all sizes, and any Canadian organizations that store personal data, to update their cyber road maps to bring them into compliance. This paper summarizes these initiatives to help CGI's clients keep pace with changing requirements and ensure their customer information is well protected.

Background

In 2010, Canada's Cyber Security Strategy established a strategic program to address growing cyberthreats. In 2015, the federal government moved to an active plan, including new legislation, and increased funding to implement the strategy.
The private sector will be affected directly by these initiatives. Chief executive officers and boards of directors are being reminded by the government of their obligation to protect the personal information of customers and employees, and the risks to their businesses if they fail to take adequate measures to protect this information.

Canada's Cyber Security Strategy was introduced with three objectives:

1. securing government systems,
2. partnering to secure vital cybersystems outside the federal government and
3. helping Canadians to be secure online. Unsurprisingly, much of the initial focus of the strategy was on improving the resiliency of the government's own systems.[1]

Over the past few years, the government has taken measures to translate these objectives into actions that included elements to support the private sector.[2] One valuable initiative has been the development of advisory documents such as:

- *Get Cyber Safe Guide for Small and Medium Businesses*[3] "to help Canadians who own or manage a small or medium business understand the cyber security risks they face, and provide them with practical advice on how to better protect their business and employees from cyber crime."
- *Industrial Control System (ICS) Cyber Security:* Recommended Best Practices,[4] a technical report "intended for IT professionals and managers within the supervisory control and data acquisition (SCADA) systems and Industrial Control System (ICS) areas of the federal, provincial/territorial and municipal governments; [private sector] critical infrastructure; and other related industries."
- *Cyber Incident Management Framework for Canada*,[5] a collaborative approach that "sets out the roles and responsibilities of all levels of government, critical infrastructure owners and operators and other public and private sector partners, in the coordinated prevention and mitigation of, preparedness for, response to and recovery from incidents affecting Canada's portion of cyberspace."

> "Today's announcement of new measures to protect vital cyber systems is encouraging."
>
> The Honourable Sergio Marchi, President and Chief Executive Officer of the Canadian Electricity Association

[1] "Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada," 2010, www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf

[2] "Action Plan 2010–2015 for Canada's Cyber Security Strategy," 2013, www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-eng.aspx

[3] "Get Cyber Safe Guide for Small and Medium Businesses," www.getcybersafe.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-eng.aspx

[4] "Industrial Control System (ICS) Cyber Security: Recommended Best Practices," 10 December 2012, www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/2012/tr12-002-eng.aspx

[5] "Cyber Incident Management Framework for Canada," August 2013, www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-ncdnt-frmwrk/index-eng.aspx

Changes Affecting Business

Among the numerous changes presented in 2015, business leaders will recall that, in January, sections of Canada's Anti-Spam Legislation came into force relating to unsolicited installation of computer programs or software.[6] Here are three other business-related cybersecurity initiatives taken by the government in 2015:

1. Digital Privacy Act provisions for mandatory reporting of security breaches
2. Intent to introduce legislation requiring operators of vital cybersystems to implement cyber security plans and report cyber security incidents to the Government
3. Increased funding to improve the Government's ability to help the private sector protect itself from cyberattacks

> "Manley said the private sector welcomed the cooperation of the federal government whose agencies can investigate cyber-attacks and prosecute cybercrime."

Below is further information on each of these initiatives, along with recommended actions for businesses.

Mandatory Reporting of Security Breaches

In 2015, the Digital Privacy Act created new legal obligations for companies that experience a security breach involving personal information. Such organizations are now required to:

- Report any breach of security safeguards involving personal information to the Privacy Commissioner if it is reasonable to believe that the breach "creates a real risk of significant harm to an individual"[7]
- Notify individuals if their personal information has been lost or stolen and there is a risk they could be significantly harmed—examples of which are identity theft, or any negative effects on their credit record[8]
- Ensure the notification is done "as soon as feasible after the organization determines that the breach has occurred"[9]
- Keep and maintain a record of these security breaches[10]

The objective of the legislation is to encourage businesses to properly safeguard personal information and to give consumers confidence that their personal information is secure. Noncompliance could be expensive, with fines of up to $100,000 for failing to notify the Commissioner or not keeping and maintaining a record of every breach of security safeguards involving personal information. In reality, damage to corporate reputations could be even more costly.

Recommended action: The Cabinet has not yet proclaimed these Digital Privacy Act breach reporting provisions to be in force, so it is unclear how they will be applied. However, the private sector needs to start thinking now about how it will comply with this new legal regime. Security information and event management systems may become increasingly important in assisting companies with their new compliance obligations.

> "The private sector is experiencing not occasional but regular, steady attacks on their cyber systems. This doesn't happen once a week or once a month, it happens on a daily and repetitive basis."
>
> The Honourable John Manley, President and CEO of the Canadian Council of Chief Executives and Co-Chair of the CEO Advisory Committee on Cyber Security

[6] Fast Facts – Canada's Anti-Spam Legislation, Government of Canada, http://fightspam.gc.ca/eic/site/030.nsf/eng/h_00039.html

[7] Bill S-4, An Act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another Act, Section 10.1(1).

[8] Section 10.1(3) and 10.1(7)

[9] Section 10.1(6)

[10] Section 10.3(1)

Vital Cyber System Legislation

Of particular note to the private sector was the Government of the day's intention to introduce "new legislation [which] will require operators of vital cyber systems to implement cyber security plans, meet robust security outcomes for their systems and report cyber security incidents to the Government of Canada."[11] A consultation process will commence once the draft legislation is released.

Recommended action: Companies that believe they are not a vital cyber system operator, and therefore not affected by the proposed legislation, may need to rethink that assumption. The National Strategy and Action Plan for Critical Infrastructure lists 10 sectors the federal government considers to be critical: health, finance, communications and IT, energy and utilities, food, water, manufacturing, transportation, safety and government. While what constitutes a vital cybersystem has not yet been defined, it likely will be some subset of these 10 sectors. A question that will need to be explored is whether a company not captured directly by the definition will be impacted by virtue of being part of the supply chain of goods or services to a vital cybersystem.

Increased Government Funding for Cyber Security Initiatives

In 2015, a number of government initiatives were directed at better protecting essential cybersystems outside the federal government through enhanced public-private collaboration and taking action against cyberattackers. These measures have been welcomed by the private sector.
The federal budget, Economic Action Plan 2015, included two announcements relating to cybersecurity that will impact the private sector. The funding approved by Parliament will continue until amended by a subsequent government and includes:

- $58 million over the next five years in new funding to further protect the Government of Canada's essential cybersystems and critical infrastructure against cyberattacks
- $36.4 million over five years in new funding to support the Government's efforts to secure Canada's vital cybersystems. The funding will not flow directly to the private sector, but rather will be used to "provide enhanced support to operators through the development and dissemination of cyber security tools, security information and expertise to implement the new legislation".[12]

[11] "Economic Action Plan," Minister of Finance, April 21, 2015, Chapter 4.3, www.budget.gc.ca/2015/docs/plan/budget2015-eng.pdf
[12] "Economic Action Plan", Minister of Finance, April 21, 2015, Chapter 4.3, www.budget.gc.ca/2015/docs/plan/budget2015-eng.pdf

In July 2015, Canada's Minister of Public Safety and Emergency Preparedness announced additional funding for cyber security initiatives to assist the private sector in dealing with cyberattacks: $142.6 million was added to the funding announced in the budget.

This additional funding will be directed to three initiatives:

1. Canadian Cyber Incident Response Centre (CCIRC)[13]
   CCIRC will see a "significant" increase in its ability to respond to, and mitigate, cyberincidents in the private sector, "including the development of real-time automated feeds of cyber threat information"[14] that will give the private sector additional threat information and faster dissemination.[15]
2. Regional Resilience Assessment Program (RRAP)
   Provides for "a site assessment project done in cooperation with the U.S. to enhance the resilience of critical infrastructure in both countries" and includes the participation of private sector facility owners and operators. "Funding will bolster the capacity of the RRAP to incorporate cyber security into the site assessment process. This measure will enable Public Safety Canada to assess the overall cyber security of an organization and provide recommendations to improve resilience."[16]
3. Law Enforcement
   The Royal Canadian Mounted Police (RCMP) will increase its capacity to detect and disrupt high-priority cybercrime through a dedicated investigative team, increased intelligence capacity, technical support and law enforcement training.

Conclusion

These federal government initiatives send a signal to businesses about the importance of a secure cyberenvironment to protect corporate and personal information. Increased funding for government programs to assist the private sector, coupled with new legal regimes relating to vital cybersystems and breaches of personal information safeguards, means that business leaders will need to pay close attention. New, additional government funding will serve to help ensure that attention.

Business leaders can expect to hear more from the government on cybersecurity. The December 2015 Prime Minister's Mandate Letter to the Minister of Public Safety and Emergency Preparedness states that one of the Minister's "top priorities" is to "lead a review of existing measures to protect Canadians and our critical infrastructure from cyber-threats."[17]

How CGI can help

As CGI's cybersecurity experts work with both the civilian and defence arms of government, as well as the private sector, we know we must stay abreast of these new realities and shifts in legislative requirements. By helping our clients adapt to these new realities, we are able to ensure that their security roadmaps and information collection policies and procedures are up to date and aligned with Canada's new laws and regulations.

[13] "The Canadian Cyber Incident Response Centre (CCIRC) operates within Public Safety Canada, and works to protect the vital cyber systems of provinces, territories, municipalities and private sector organizations. CCIRC produces a range of publically available technical advice and guidance products to assist cyber security professionals in securing their businesses," **www.getcybersafe.gc.ca/cnt/prtct-yrslf/prtct-smlbsn/index-en.aspx**

[14] Government of Canada, Public Safety Canada, Backgrounder, "Advancing Canada's Cyber Security Strategy"; and CBC News, July 22, 2015, "Steven Blaney announces new funding for cyber security" by Susana Mass

[15] Government of Canada, Public Safety Canada, Backgrounder, "Advancing Canada's Cyber Security Strategy"; and ITWorld Canada, July 22, 2015, "Ottawa increases spending to protect critical infrastructure from cyber attacks," by Howard Solomon.

[16] Ibid

[17] "Minister of Public Safety and Emergency Preparedness Mandate Letter, **http://pm.gc.ca/eng/minister-public-safety-and-emergency-preparedness-mandate-letter**

cgi.com

Founded in 1976, CGI is one of the largest IT and business process services providers in the world, delivering high-quality business consulting, systems integration and managed services. With a deep commitment to providing innovative services and solutions, CGI has an industry-leading track record of delivering 95% of projects on time and within budget, aligning our teams with clients' business strategies to achieve top-to-bottom line results.