# MORE CHANGES TO CYBER SECURITY LAWS ON THE HORIZON?

*Posted on July 15, 2015*

**Categories:** Insights, Publications

The issue of cyber security has become increasingly topical as more and more business, government and personal interactions occur online. Organizations that routinely collect and store user information, such as credit card or other financial information, have become targets for cyber criminals seeking to breach security measures and access such information. Some of the recent high profile breaches that relate to theft of financial information, like the breach of Target Corporation's systems and subsequent loss of massive amounts of user data in late 2013, are only one facet of cyber attacks. Cyber attacks may also be aimed at healthcare as well as infrastructure such as energy, finance, telecommunications, transportation and water.

With the release of the *Federal Budget* in April, the Government of Canada (GOC) has recognized these risks and reaffirmed its commitment to promoting cyber security in Canada in both the public and private sectors.

Under the chapter heading of "Protecting Canadians", the GOC outlined various initiatives related to national security and defence, ranging from border protection initiatives to expand simplified entry for low-risk travellers to the National Defence budget for Canadian Armed Forces.

Included in this same section, as part of the broader goal of enhancing national security, the GOC allocated nearly $100 million over the next five years toward protecting the GOC's "essential cyber systems and critical infrastructure against cyber attacks" and supporting "operators of Canada's vital cyber system in addressing cyber security threats".

**Government Systems**

The Budget includes $58 million for upgrading critical government cyber systems, including Internet network paths and connections. The stated purpose of these upgrades is to ensure that such critical systems can be protected through detecting and repelling infiltration attempts on GOC systems, and also identifying malicious actors.

**Private Systems**

On the private side of the equation, the GOC has acknowledged that Canadians gain daily advantage from use of online systems and services, and that this increasing reliance on such networked resources makes us "more

vulnerable to those who would seek to attack and undermine our digital infrastructure and threaten our national security, economic prosperity and way of life".

The Budget provides that the GOC plans to introduce new legislation which will require operators of "vital cyber systems" to implement security plans, meet "robust" security requirements, and report cyber security incidents to the GOC. This new legislation is currently being called the *Protection of Canada's Vital Cyber Systems Act* (the "**Cyber Act**"), which has been in the works for some time, but has yet to be officially introduced.

In order to support the enhancements required of individual operators by the Cyber Act, the Budget provides $36.4 million to provide enhanced support through the development and dissemination of cyber security tools, security information and expertise to implement the new legislation.

**Canada's Cyber Security Strategy**

These cyber security announcements in the Budget represent implementation of Canada's *Cyber Security Strategy*, released in 2010, which was built upon the following three pillars:

- **Securing Government systems** – The GOC needs to maintain the trust of Canadians with both personal and corporate information.
- **Partnering to secure vital cyber systems outside the federal government** – Many (if not most) of the modern advantages that Canadians rely upon originate from private industry.
- **Helping Canadians to be secure online** – In addition to infrastructure and systems, public information is key to enable Canadians to protect themselves and their families online.

**Protection of Canada's Vital Cyber Systems Act**

While the Budget, particularly when read in connection with the Cyber Security Strategy, gives an indication of the principles underlying the Cyber Act, an analysis of the actual impact of the Cyber Act on industry and individual operators will not be possible until the Cyber Act is tabled as a Bill before Parliament.

One crucial issue to be addressed will be the definition of "vital cyber systems". It is likely that the Cyber Act will at least focus on organizations responsible for the Internet-infrastructure in Canada, such as telecommunications companies and Internet service providers. However, the online economy continues to move further into the cloud, with the result that Canadians are becoming more reliant on web and mobile-based services and service businesses are becoming increasingly dependent on various networks to deliver efficient services. Therefore, the GOC may choose to expand the scope of responsibility for cyber security under the Cyber Act beyond the typical infrastructure providers.

However, with Parliament currently adjourned until late September, and an election scheduled to occur October 19, 2015, the future of the Cyber Act is uncertain.

What is certain, is that organizations that have control over sensitive personal information or essential public or private systems would be well-advised to review the state of their cyber security, to determine whether they are vulnerable to threats and/or complying with any applicable legal requirements. For more information on cyber security, please see McMillan's Privacy Basics Issue #4, *Cybersecurity*.

by Lyndsay A. Wasser and Michael Reid

**A Cautionary Note**

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.