ARE CANADIAN BUSINESSES READY FOR A CYBER ATTACK?

Posted on April 3, 2017

Categories: Insights, Publications

On April 3, the Canadian Chamber of Commerce ("**CCC**") released a white paper titled "Cyber Security in Canada,"[1] (the "**Report**") which examines the current Canadian cyber landscape, the cyber readiness of Canadian businesses, the current state of cyber insurance, and also releases a set of recommendations for the Canadian government to consider regarding cyber security.

"Cyber Security" Definition and Classification Systems. The white paper explains that "cyber security" is "the protection of computer systems from theft or damage to the hardware, software or the information on them, as well as from disruption or misdirection of the services they provide."[2] The Report states that the hierarchy of cyber targets is based on the data's value (defined by sensitivity and volume), and targets fall into four general categories: 1) national security, 2) critical infrastructure, 3) intellectual property, and 4) personal data. Similarly, the Report indicates that cyber threats can be grouped into three categories: 1) confidentiality (e.g. of private information), 2) availability (e.g. service access and data deletion), and 3) integrity (e.g. virus and malware infections). The Report categorizes attackers into two categories (state and non-state actors), or more refined categories such as state sponsored actors, organized crime, and hacktivists. Despite these variations, the Report indicates that most cyber attacks take the path of least resistance and thus share three basic characteristics: they are 1) inexpensive, 2) effective, and 3) low risk.

The Cyber Landscape. The Report finds that cyber crime is "becoming a preoccupation in corporate board rooms," forcing consideration of three core risk management questions: 1) what is at stake, 2) who is after it, and 3) what can they do to protect their interests. This is partly in response to an increase in "businesses reporting a loss or exposure of sensitive data" (8% in the past 3 years).[3] In Canada in particular, businesses reporting no losses from cyber crime decreased from 45% to 40% in 2016.[4] Further, the number of businesses reporting a CAD $1 million plus loss has risen to 7% from 1% just two years ago.[5] The Report notes, however, that there is little international alignment, and that focus has been on compliance instead of risk-based security performance.

Cyber Insurance. In response to the increase in cyber attacks, the Report indicates that there has been a "dramatic growth of the cyber insurance industry,"[6] and the value of "premiums for cyber liability policies is expected to triple by 2020, rising to $7.5 billion USD."[7] Of note, the greatest share of claims made on such

policies come from the health sector, at 40% of the share of cyber liability claims made in the US in 2014.[8] Insurance is expected to remain a necessary consideration in cyber risk management as "there is a need to accept the inevitability of defeat."[9]

Round Table Results. In October 2016, the CCC brought together thought leaders from across Canada. Overall, the consensus was that more information and guidance is necessary, especially for small and medium-sized enterprises ("**SMEs**") regarding cyber security. It was also noted that, although humans are the best resource in fighting cyber attacks, they are also the weakest link in terms of resilience. The discussions revealed that many of the current robust guidelines, such as the ISO-27001 certification standard and the ISO-27032 cyber security guideline, are too costly for many businesses, and so the CCC has partnered with the International Cyber Security Protection Alliance ("**ICSPA**") to deliver a cost effective and achievable certification standard.[10]

The discussions also mentioned the emerging privacy legislation regime focused on businesses that collect and store personal information, and the related tensions for adapting businesses. While all companies are potential targets for cyber attacks, the discussions highlighted that many companies lack the ability to recognize and adequately respond to breaches. The consensus is that accountability and ownership of solutions is crucial. Finally, the round table discussion highlighted the government's role, including facilitating improvements to business responses through, for example, tracking fraud and making enforcement a priority, appointing a single ministry or agency to oversee a cyber file, and adopting a robust cyber security strategy.

The SME Factor. Small business is important to the Canadian economy. The Report notes that 71% of data breaches happen to small businesses,[11] and although SMEs know they need to do more to protect themselves, they do not know how. The Report states that SMEs attract criminals because: 1) SMEs are less equipped to handle attacks, 2) their valued information is often less guarded, and 3) the SME partnerships provide backchannels to higher-value targets.[12] A survey conducted by the CCC in February 2017 found that, while Canadian SME's use of anti-malware and firewalls is better than in the US, they lag behind larger businesses for other measures.

Results of Workshops - Survey. The CCC conducted a survey of approximately 260 businesses across the country to find out what cyber security tools they were using. The majority of businesses (both small and large) use both firewalls and regularly back up their data. However, there appears to be a wide discrepancy between SMEs and mid-to-large sizes business in the adoption of additional cyber security tools such as VPN, multi-factor authentication, encryption software, network visibility tools, etc.

Results of Workshops – Health Checks. The CCC also asked 75 businesses across Canada to respond to five cyber "health checks," in areas including technology, public relations, cyber awareness, legislative compliance and cyber insurance.

Technology Check. The technology check found that while the majority of businesses have identified their critical assets (69%)[13], they do not know how to prioritize the protection of their critical assets (55%)[14] or whether they have sufficient technology to protect those critical assets (57%)[15].

Public Relations Check. The public relations check found that the majority of businesses have not put in place a cyber security plan (82%)[16] nor have they thought through how to handle the public relations component of a cyber security incident.

Cyber Awareness Check. The cyber awareness check found that almost half of all businesses have some understanding of their cybersecurity risk and obligations. For example, 50%[17] of businesses have cyber use policies, 62%[18] of businesses stated that their protocols for data sharing with partners are followed, and 60%[19] have organizational cyber education programs.

Legislative Compliance Check. The legislative compliance check raised concern as approximately half of businesses queried indicated that they did not know or understand their obligations required under the Personal Information Protection and Electronic Documents Act ("**PIPEDA**"). Specifically, only 56%[20] of respondents indicated that they are aware and compliant with schedule 1 of PIPEDA. Additionally, of great concern is that only 18%[21] of respondents were aware if personal data was stored in Canada.

Cyber Insurance Check. The cyber insurance check found that only 26%[22] of businesses have cyber liability coverage, 29%[23] have data restoration coverage, 35%[24] have coverage for losses from third part cloud services and 26%[25] have coverage for lawsuits relating to a data breach. What this shows is that Cyber security is not well known and is underutilized as a risk management tool.

Discussion. The Report's discussion suggests considerations for businesses when instituting cyber security policies, including evaluating the value and sensitivity of their data. The easiest method for businesses is to regularly back-up their data and store it outside the business network. Businesses should also consider information-sharing to improve their cyber security. The Report gives two examples of means already in place: "CCTx," which is an independent not-for-profit organization that shares information about cyber threats and vulnerabilities, and "FIRST," which is a membership exchange platform for exchanging information on cyber incidents, best practices, and tools and methodologies for strengthening cyber security. The Report also discussed future technology with the potential to make big changes, such as tokenization, blockchain, the "internet of things," or quantum computing.

Government Recommendations. The Report made the following recommendations: 1) government implementation of a P3/coordinated approach to improving cyber security; 2) implement cyber security policies which are outcome-based; 3) develop a secure, shared-leadership, national approach to privacy and security; 4) implement a national cyber policy supporting cyber innovation and risk detection; 5) develop a

security baseline framework for cyber risk management across economic sectors in partnership with G20 nations; 6) invest in digital literacy and technological awareness to increase "cyber savviness"; 7) support for / Endorsement of an industry certification program across multiple sectors (such as the one currently deployed in the United Kingdom); 8) government implementation of incentives for incorporation of cyber security features; 9) ensure that any strategies implemented should be "quantum-ready".

by Jeffrey Nagashima and Kailey Sutton, Student-At-Law

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.

[1] The Canadian Chamber of Commerce, "Cyber Security in Canada" (April 3, 2017) available online at: http://www.chamber.ca [Cyber Security in Canada].
[2] Cyber Security in Canada, *supra* note 1, page 8.
[3] 2017 Scalar Security Study, "The Cyber Security Readiness of Canadian Organizations" (2017) available online at: https://media.scalar.ca.
[4] Cyber Security in Canada, *supra* note 1, page 14.
[5] Cyber Security in Canada, *supra* note 1, page 16.
[6] Cyber Security in Canada, *supra* note 1, page 17.
[7] Forbes, "Cyber Insurance Market Growing From $2.5 Billion In 2015 To $7.5 Billion By 2020" (December 24, 2015), available online at: http://www.forbes.com.
[8] Marsh & McLennan Agency, "Cyber & Data Security Risk Survey" (November 2014), available online at: http://information.rjfagencies.com.
[9] Cyber Security in Canada, *supra* note 1, page 20.
[10] Note also that CyberNB has partnered with ICSPA to build out a number of related platforms.
[11] Cyber Security in Canada, *supra* note 1, page 25.
[12] *Ibid*.
[13] Cyber Security in Canada, *supra* note 1, page 31.
[14] *Ibid*, page 31.
[15] *Ibid*, page 31.
[16] *Ibid*, page 32.
[17] *Ibid*, page 33.
[18] *Ibid*.

[19] *Ibid*.
[20] Cyber Security in Canada, *supra* note 1, page 34.
[21] *Ibid*, page 34.
[22] *Ibid*, page 35.
[23] *Ibid*, page 35.
[24] *Ibid*, page 35.
[25] *Ibid*, page 35.