April 2017

The tides are changing for cyber regulation, and you may need to take action in order to stay afloat

In 2017 businesses will see significant changes to the cyber regulatory landscape, and Canadian businesses' cyber protocol will have to adapt accordingly.

This bulletin focuses on two areas of anticipated change. First, securities regulators are stressing the need for issuers to disclose their cybersecurity risks and incidents in their Annual Information Forms, MD&A and other continuous disclosure documents. Second, the new Canadian anti-spam regulations will now permit private actions to be pursued for the sending of commercial electronic messages. These two examples illustrate the diverse ways in which Canadian businesses will need to critically re-assess their cyber activities to respond to changing cyber regulation.

Issuers' disclosure of cybersecurity risks and incidents

Since the Canadian Securities Administrators (**"CSA"**) identified cybersecurity as a priority in their 2016-2019 Business Plan, a number of Staff Notices have been published to provide guidance for issuers on the disclosure of their cybersecurity protocols.[1] Based on an assessment of the disclosure practices of 240 reporting issuers, the CSA found that 40% of issuers did not identify cybersecurity as a

[1] CSA Multilateral Staff Notice 51-347 – Disclosure of cybersecurity risks and incidents; CSA Staff Notice 11- 332 – Cybersecurity.

material risk in their continuous disclosure documents. Considering the rate at which the detection of security incidents has increased, these statistics suggest that reporting issuers are not acknowledging and/or disclosing their vulnerabilities to cybersecurity risks.

The low rate of disclosure may be attributed to the fact that there is no explicit requirement in Canadian securities law for the disclosure of cybersecurity risks; rather, the requirement is that all material risks be disclosed, with materiality being defined as information that a reasonable investor would consider important when deciding whether to invest. As data breaches are becoming more commonplace, and gaining higher profiles, cybersecurity is expected to become increasingly material to investors.

For example, Yahoo's handling of their 2013/2014 cyber attacks illustrates how data breaches, public opinion, and securities regulators can become intertwined. Not only did Yahoo's data breach and public outcry jeopardise their estimated $4.8 billion deal with Verizon, it also led to Verizon receiving a $350 million offset for damages. Subsequently, the U.S. Securities Exchange Commission opened a formal investigation in December 2016 to assess whether Yahoo's disclosure to investors ought to have occurred earlier.[2]

While there have only been a limited number of reported data breaches, this is likely to change as well. Issuers should be aware that the long-awaited *Digital Privacy Act*[3] regulations will likely come into force by the end of this year.[4] It is anticipated that these regulations will require organizations to maintain a record of all breaches, and notify users of any breach that could pose "a real risk or significant harm" to any individual whose personal information was involved in the breach. A failure to handle breaches in accordance with the regulations could result in fines of up to $1,000,000. This means that news of data breaches will garner higher profiles and

---

[2] Aruna Viswanatha and Robert McMillan , "Yahoo Faces SEC Probe Over Data Breaches", Wall Street Journal, January 23, 2017. https://www.wsj.com/articles/yahoo-faces-sec-probe-over-data-breaches-1485133124.

[3] *Digital Privacy Act*, SC 2015, c.32.

[4] https://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf11177.html; http://betakit.com/data-breach-reports-set-to-skyrocket-in-2017-thanks-to-passing-of-digital-privacy-act/.

greater backlash. In 2016, not one of the 240 studied issuers claimed they had a material breach. This is unlikely for 2018 as the new regulations come into effect.

In light of this, issuers should revisit the mechanisms used to assess their disclosure of material risks and what might constitute a material change or fact to merit disclosure. In particular issuers should be aware of the following when preparing risk and incident disclosures:

- Risk Disclosure: Entity specific and non-boilerplate descriptions of why issuers are exposed to potential breaches, the source and nature of risk, the consequences of a breach, the preventative measures and any mitigation steps will assist issuers in asserting sufficient information was disclosed.

- Incident Disclosure: While there is no bright line test to know when a data breach constitutes a material change or fact, issuers need to realise that the assessment is a dynamic one and something that is not initially identified as a material change or fact could become one with time. Designating a body, such as the audit committee, to monitor the situation can assist in this process.

In short, issuers need to shift from being reactive to proactive.

Trigger clicking: think before you click

As of July 1, 2017, individuals and organizations can bring a "private right of action" before the courts against those organizations that contravene Canada's Anti-Spam Law[5] ("**CASL**"). CASL regulates the sending of commercial electronic messages ("**CEMs**") and requires individuals and entities that distribute CEMs to obtain prior consent (direct or implied) from intended recipients.

Given the increase in potential liability, issuers should ensure their policies and procedures are in compliance with CASL.

---

[5] *An Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying out Commercial Activities, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act,* SC 2010, c 23.

- First, firms must have a clear understanding of the breadth of the legislation and how their existing communication with clients can be captured under the law. The broad definition of CEMs is "an electronic message that encourages participation in a commercial activity, regardless of whether there is an expectation of profit", this includes e-mails, texts, instant messages, and social media messages sent to the electronic addresses of clients.

- Second, firms should ensure that a clear and comprehensible CASL policy is in place. The policy should delineate the types of communications requiring consent, the processes that must be followed to collect consent from clients, and specify how consent is recorded.

- Third, the policy should also detail the mechanism to deal with client complaints and how these are addressed. The existence of a policy is increasingly important with the private "right of action" coming into force seeing as organizations can employ a due diligence defence when accused of a violation under CASL.

The potential liability of a private right of action is in addition to the existing enforcement by the Canadian Radio-television and Telecommunications Commission (CRTC), the Competition Bureau and the Office of the Privacy Commissioner of Canada.

CASL infringement is not a small risk by any measure. Court ordered damages can be of up to a $1,000,000 for each day on which a contravention occurred, and the CRTC has already imposed penalties in the millions of dollars. With a few months to go, this is the perfect time to ensure compliance with CASL. For more information visit our bulletin on this issue.

Conclusion

As cyber regulation tries to catch up with the cybersecurity crises that has been picking up steam over the past decade, issuers should review their cybersecurity protocols to ensure compliance with the array of new requirements.

by Jason A. Chertin, Maria Valdivieso and Christie Bates (Student-at-Law)

For more information on this topic, please contact:

Toronto	Jason A. Chertin	416.865.7854	jason.chertin@mcmillan.ca
Toronto	Maria Valdivieso	416.945-8020	maria.valdivieso@mcmillan.ca

a cautionary note