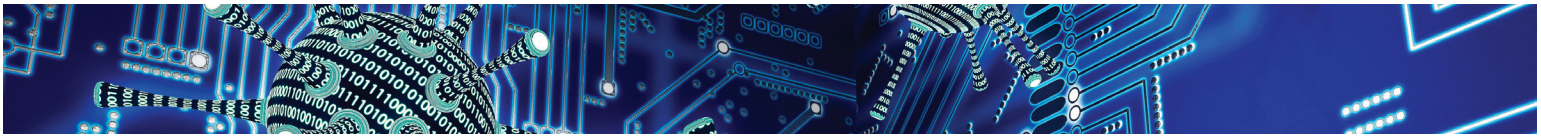

CSA ISSUES CYBERSECURITY DISCLOSURE EXPECTATIONS

By: Imran Ahmad, Peter Dunne & Pierre Soulard

Increasingly, cybersecurity is a top of mind issue for most organizations. Senior management, board members and investors are particularly concerned given the potential negative impact a major cyber-attack can have on organization from a financial, legal, reputational and operational standpoint.

It is therefore no surprise that the Canadian Securities Administrators (the "**CSA**") has been active in the area of cybersecurity in recent months. Last week, it issued Staff Notice 51-347 (the "**Notice**"), an updated notice on cybersecurity expectations for issuers regarding the disclosure of cybersecurity risks and incidents. The Notice also includes a summary of the CSA's review of the most recent annual filings of 240 constituents of the S&P/TSX Composite Index, focusing on whether and how issuers addressed cybersecurity issues in their risk factor disclosure.

Disclosure Trends

The CSA's review of issuers' cybersecurity disclosure found that nearly 40% of issuers failed to address cybersecurity issues in their risk factor disclosure. Those that did provide such disclosure, generally indicated that dependence on information technology systems presented a risk for cybersecurity breaches. Few issuers addressed their particular vulnerability to cybersecurity incidents and risks caused by third parties.

The CSA noted that the potential impacts of a cybersecurity incident most commonly cited by issuers included: loss of revenue; business disruption; litigation exposure, fines, and liability; regulatory investigations and increased regulatory scrutiny; higher insurance premiums; reputational harm; and loss of investor confidence; etc.

Disclosure of Cybersecurity Risk

The Notice also provides guidance on best practices for risk factor disclosure:

- **Avoid boilerplate language.** Disclosure should emphasize information that is entity-specific, given that the purpose of disclosure is to allow readers to distinguish issuers from one another.
- **Likely types of threats.** Issuers should consider the type of cyber-attacks they may experience and the ways in which cyber-attacks will be conducted. Though all issuers may be exposed to risk of an attack, issuers will be affected differently. For example, an e-commerce platform may experience an attack that denies service to consumers. While this type of attack may be fatal to a consumer-facing issuer, the impact on a manufacturing issuer might be less severe.
- **Material risks.** Materiality turns on the probability that a breach will occur and the estimated magnitude of its effect. If cybersecurity is determined to be a material risk, disclosure should be as detailed and entity-specific as possible.
- **IOSCO factors.** The factors identified by the International Organization of Securities Commissions should also be considered by issuers. These factors include: the reason a breach may occur; source of risks; potential consequences; adequacy of preventative measures; prior material cybersecurity incidents; how risk is mitigated; and governance issues.
- **National Instrument 52-109.** Issuers required to create disclosure controls and procedures under National Instrument 52-109 *Certification of Disclosure in Issuers' Annual and Interim Filings* should include detected cybersecurity incidents. This is to ensure management is informed of incidents and is able to decide whether and what to report in a timely manner.

Disclosure of Cybersecurity Incidents

In considering whether and when to disclosure a cybersecurity incident, issuers must first determine whether it is a material fact or material change that requires disclosure in accordance with securities legislation (the "**materiality threshold**"). Materiality depends on a contextual analysis of the incident. For example, an isolated attack may not be material, though a series of small breaches may be considered material depending on the ultimate disruption caused. The Notice also emphasizes the importance of the timing of material incident reporting, though it acknowledges that it may take time to identify the occurrence of a breach and to fully assess its consequences.

Issuers are expected to establish cyber-attack remediation plans that address how the materiality of a breach would to assessed to determine whether, what, when, and how an incident should be disclosed.

Key Takeaways

As cyber-attacks become the new norm, issuers must carefully assess their cybersecurity risks and make appropriate disclosures.

It appears that cybersecurity is a priority area for the CSA and will continue to be so for the foreseeable future. Recent action taken by the CSA is consistent with the steps taken by other international securities regulators. Of particular interest is the increased enforcement action by the U.S. Securities Exchange Commission with respect to cybersecurity disclosures in public filings.

In light of the Notice, issuers should take the time to identify specific cyber risks that are the most relevant and likely to impact their organization. This may require bringing external consultants and experts who can provide a cyber risk profile for the organization. This understanding of the cyber risk profile will inform organizations whether the materiality threshold is triggered and if so, tailor its cyber risk and incident disclosure language accordingly.

1 The authors would like to thank articling student Victoria de Luna for her assisting in preparing this article.

Contacts

Imran Ahmad
416.597.6031
iahmad@millerthomson.com

Peter Dunne
416.597.6034
pdunne@millerthomson.com

Pierre Soulard
416.596.2127
psoulard@millerthomson.com