January 2017

CSA Provides Cybersecurity Risk Disclosure Guidance and Best Practices for Reporting Issuers

In a recent bulletin, we discussed the Canadian Securities Administrators' (CSA) Staff Notice 11-332 *Cyber Security* published on September 27, 2016, in which the CSA noted recent trends in the cybersecurity landscape and proposed policy initiatives to help market participants reduce their exposure to cybersecurity risk. The CSA also indicated that CSA members would examine the filings of some larger issuers to analyze their risk disclosure with respect to cybersecurity attacks.

On January 19, 2017, the CSA published Multilateral Staff Notice 51-347 *Disclosure of cyber security risks and incidents* (the 2017 Notice) to report the findings of the CSA's review of the 240 constituents of the S&P/TSX Composite Index and provide disclosure expectations for reporting issuers. The 2017 Notice indicates that 61% of the reviewed issuers addressed cybersecurity risk in their risk factor disclosure and that issuers in a wide variety of industries acknowledged cybersecurity as a material risk.

However, the 2017 Notice remarks that very little of the disclosure reviewed actually included disclosure of an issuer's particular vulnerability to cybersecurity incidents. The CSA directs issuers to avoid boilerplate language when disclosing their exposure to cybersecurity risk and instead disclose material and entity-specific information. The risk disclosure resulting from such an analysis should be as detailed as possible so that readers can distinguish one

issuer from another, in the same industry or across industries, with respect to level of exposure, cybersecurity preparedness, and how cybersecurity risk materially impacts the issuer. At the same time, an issuer's risk disclosure should not compromise its security or reveal sensitive information.

The CSA expects all issuers to consider the following factors when preparing their disclosure:

- the reasons they may be exposed to a cybersecurity breach;
- the source and nature of the risks;
- the potential consequences of a breach;
- the adequacy of preventative measures; and
- any prior material cybersecurity incidents and their effects on cybersecurity risk.

Further, the CSA expects issuers to address how they mitigate any risk identified (including the extent of reliance on cybersecurity insurance and third party experts), as well as discuss any governance issues relating to their internal development of cybersecurity risk management.

The CSA has recognized that not all issuers are affected by cybersecurity risk in the same ways or to the same extent. As in all types of risk factor disclosure, the issuer must consider whether the cybersecurity risk it faces is material to its business, based on an analysis of the probability that a breach will occur and the anticipated magnitude of its effect if it does. The CSA further recognized that because there is no "bright-line test" for materiality, the analysis is context-specific and must be applied to each cybersecurity incident.

The CSA compiled both industry-specific and industry-agnostic lists of potential impacts from a cybersecurity incident, taken from their review of issuer disclosure. Interestingly, the list of industry-agnostic impacts is the larger of the two. A review of these potential impacts,

as follows, provides a good reminder that cybersecurity risk assessment is important for all organizations in all industries:

- compromising of confidential customer or employee information;
- unauthorized access to proprietary or sensitive information;
- destruction or corruption of data;
- lost revenues due to a disruption of activities;
- incurring of remediation costs;
- litigation, fines and liability for failure to comply with privacy and information security laws;
- regulatory investigations and heightened regulatory scrutiny;
- higher insurance premiums;
- reputational harm affecting customer and investor confidence;
- diminished competitive advantage and negative impacts on future opportunities; and
- effectiveness of internal control over financial reporting.

Ultimately, cybersecurity disclosure must be tailored to each issuer. In this ever-changing and developing landscape, issuers should seek legal advice to evaluate their current cybersecurity risk disclosure strategy. Counsel can also advise issuers on how materiality of an attack could be assessed to determine the appropriate amount of disclosure to make following a cybersecurity attack, keeping in mind that other laws, in addition to securities regulation, may require an issuer to disclose particulars of a breach.

by Arman G. Farahani, Rohan Hill and Bill Olaguera, Articled Student

For more information on this topic, please contact:

Vancouver	Arman G. Farahani	604.691.7430	arman.farahani@mcmillan.ca
Vancouver	Rohan Hill	778.328.1492	rohan.hill@mcmillan.ca

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.