Expectations for Cyber Security Risk Disclosure Published by CSA

February 21, 2017

Vanessa Coiteux, Jérémie Ste-Marie

The results of the Canadian Securities Administrators' (CSA) review of the cyber security risk disclosure of S&P/TSX Composite issuers were recently reported by the the *Autorité des marchés financiers*, the Ontario Securities Commission and the British Columbia Securities Commission in **CSA Multilateral Staff Notice 51-347** (the Notice). Focused particularly on risk factor disclosure and disclosure of cyber security incidents, the CSA's review follows last year's publication of **CSA Staff Notice 11-332 Cyber Security**, which reiterated that cybersecurity would continue to be one of the **CSA's priorities through 2019**.

Risk Factor Disclosure

With respect to risk factor disclosure, the CSA focused on three topics:

- the disclosure of the risk itself,
- the disclosure of potential impacts of a cyber security incident, and
- the disclosure of governance practices and cyber security risk mitigation.

The CSA found that 61% of issuers reviewed included cyber security risks in their disclosure. Issuers generally disclosed that their dependence on information technology systems puts them at risk for cybersecurity breaches and that they consider cyber security as a material risk to their organization. However, only a few issuers disclosed particulars regarding their cyber vulnerability, which would include, for example, how they are vulnerable compared to other issuers operating in the same sector or factors that could increase their vulnerability.

The CSA provided guidance for risk factor disclosure:

- Disclosure should focus on material and entity specific information, avoid boilerplate language and focus on an issuer's particular circumstances. The CSA expects disclosure to help investors distinguish cyber risks that are specific to the issuer as compared to other issuers in terms of level of exposure, level of preparedness and how the risk impacts the issuer.
- Issuers should consider the types of cyber-attacks to which they may be exposed as well as the manner of such exposure. The CSA does not expect issuers to disclose details regarding their cyber security strategy or their vulnerability to cyber-attacks that is of a sensitive nature or that could compromise their cyber security. **As previously discussed**, finding the right balance between disclosing all relevant and material facts to an investor, while making sure

not to provide a roadmap to an issuer's vulnerabilities, may not be a simple task. There is a thin line between insufficient disclosure and excessive disclosure. It will be interesting to see whether and if so, how, issuers will use the "sensitivity/prejudicial" exception to explain their lack of specificity in terms of cyber risk disclosure, and what the CSA will do in response, including whether it will publish more guidelines or establish a framework to help issuers determine whether or not a risk or a fact needs to be disclosed.

- In preparing cyber security risk factor disclosure, issuers should consider, and to the extent applicable include, details regarding the source and nature of the risks, the potential consequences of a cyber security breach, the adequacy of preventive measures, how they mitigate the risk (including through cyber-insurance or reliance on third party experts), their governance structure and the entity responsible for the issuer's cyber security, as well as any risk mitigation strategy, for example, incident response plan, cyber security policy, or employee training.
- The CSA expects issuers who are required to establish and maintain disclosure controls and procedures under National Instrument 52-109 *Certification of Disclosure in Issuers' Annual and Interim Filings* to apply such controls and procedures to detected cyber security incidents so as to ensure that those incidents are properly communicated to management and that a decision regarding whether and how to report such incident is made in a timely manner. In response to growing market demand for information about the effectiveness of an entity's cyber security risk management program, the American Institute of Chartered Public Accountants is **developing a new engagement** that Chartered Public Accountants can use to assist boards of directors, senior management, and other pertinent stakeholders as they evaluate the effectiveness of an entity's cybersecurity risk management program.

Cyber Security Incidents Disclosure

While a **recently published survey** has suggested that cyber security incidents in Canada have significantly increased over the last few years, the CSA found that none of the 240 issuers surveyed disclosed that they had been subject to a cyber-attack that they considered material. Not surprisingly, the foregoing **is consistent with practices in the United States** where, since 2010, only 95 of the U.S.'s 9,000 publicly listed companies have informed the SEC of a data breach while the number of breaches or hacks across all U.S. businesses totaled 2,642 during the same period.

As discussed in the Notice, privacy or other legislation may require issuers to report or notify individuals of cyber security breaches while not necessarily triggering an obligation to disclose those same incidents under securities legislation. In performing their assessment as to whether a cyber security incident must be disclosed in their public disclosure, issuers should rely on the traditional materiality tests set by securities law as well as case law to determine whether a cyber incident constitutes a "material fact" or a "material change" and if so, when the incident should be disclosed. Reference should be made to National Policy 51-201 *Disclosure Standards* for guidance on this determination.

The CSA also indicates that, in their determination as to whether a cyber-incident is "material", issuers should notably take into account:

- the timing of the cyber incident;
- the importance of the breach for the Issuer (price tag associated with the breach compared to the Issuer's revenue, profits, etc.); and
- the involvement of personal, confidential or sensitive information.

With respect to the timing of the disclosure, the CSA acknowledges that cyber security incidents may not be detected until long after their occurrence, and the consequences of the incident may take time to fully assess. The determination of whether the incident is material is a dynamic process to be completed throughout the detection, assessment and remediation phases of a cyber security incident.

Whether or not a cyber security incident is reportable under securities laws is a judgment call that has to be made by each issuer. However, those decisions are likely to be scrutinized by investors and regulators who have been advocating for more disclosure in that respect. It will therefore be interesting to see whether and how institutional investors and regulators may increase pressure on cyber incident disclosure in the next proxy season. In the United States, even though the SEC has not yet filed a regulatory enforcement action against any issuer that has failed to disclose a cyber incident, it has nonetheless sent several comment letters to multiple large reporting issuers concerning their disclosure of cyber incidents, notably requesting further elaboration on whether data breaches had occurred, how companies responded to such breaches, and additional information as to why some companies believe that the breaches they suffered were not sufficiently material to warrant disclosure. With the notification provisions of cyber incidents that will soon be in force under *the Personal Information Protection and Electronic Documents Act* (PIPEDA) and the resulting knowledge of actual cyber incidents within the public realm, we can expect such scrutiny to increase.