Goodmans LLP Update

Corporate Securities and Technology Law

January 24, 2017

CSA Provides Guidance on Disclosure of Cyber Security Risks

On January 19, 2017, the Canadian Securities Administrators (CSA) published Multilateral Staff Notice 51-347 *Disclosure of cyber security risk and incidents* (the "**Staff Notice**") reporting on the CSA's review of cyber security-related disclosure. The notice is part of a series of initiatives being undertaken by Canadian securities regulators to assist market participants in understanding, mitigating and providing effective disclosure of potential cyber security risks.

CSA Staff Review of Cyber Security Disclosure

Cyber security was identified as a priority area by the CSA in their 2016-2019 Business Plan. In September 2016, the CSA published Staff Notice 11-332 *Cyber Security*, which noted that cyber attacks have become more frequent, complex and costly for organizations. In that context, the CSA announced that it would undertake a review of cyber security-related disclosure by larger Canadian issuers. The CSA's review focused on whether and how issuers had disclosed (1) potential impacts of cyber attacks on their businesses, (2) the kind of material information that could be exposed as a result of attacks, and (3) governance and cyber security risk mitigation initiatives, including who is responsible for the issuer's cyber security strategy. The review also searched for disclosure of previous cyber security incidents.

The CSA noted that 61% of the issuers reviewed addressed cyber security in their risk factor disclosure and that issuers in a wide variety of industries acknowledged cyber security as a material risk to their business. Issuers recognized a range of potential impacts from cyber security incidents, including:

- access to, and/or comprising of, proprietary or sensitive information, including confidential customer or employee information;
- loss of revenues due to disruption of business activities;
- litigation and regulatory costs;
- reputational harm affecting customer and investor confidence; and
- devaluation of intellectual property.

The CSA also noted that while a few issuers disclosed that they had been subject to cyber attacks in the past, no issuers had disclosed specific incidents as being material.

CSA Staff Guidance for Issuers

Not surprisingly, the CSA Staff expects issuers to be thoughtful about the cyber security risks they are subject to, to avoid boilerplate language and to provide disclosure that focuses on material information that is specific to the issuer. CSA members expected that to the extent issuers have determined that cyber security risk is a material risk, they will provide risk disclosure that is as detailed and "entity specific" as possible. There is an express expectation that specific risks will be disclosed, rather than generic risks applicable to all issuers, and that disclosure will be tailored to the specific circumstances of the issuer.

In preparing risk factor disclosure regarding cyber security matters, the CSA expects that issuers will consider (among other things):

- the reasons they may be exposed to a potential breach;
- the source and nature of the breaches;
- the potential consequences of the breach;
- insurance coverage in case of the breach;
- identifying the group or individuals responsible for the issuer's cyber security; and
- where required, apply disclosure controls and procedures under National Instrument 52-109 *Certification of Disclosure in Issuers' Annual and Interim Filings* to detected cyber security incidents.

At the same time, the CSA does not expect issuers to disclose sensitive information that could compromise their cyber security risk mitigation strategies.

The CSA also reminds issuers to consider whether a specific security incident might be a material change that requires immediate disclosure or a material fact that requires disclosure as part of issuers' ongoing reporting obligations. Materiality in this context depends on the circumstances of the security breach. For example, an isolated minor breach may not be material but a series of minor breaches may become material in light of the level of disruption caused. The determination of whether an incident is material is a dynamic process through the detection, assessment and remediation process of a cyber security incident and depending on the circumstances, disclosure could be required before that process is complete.

In light of the CSA's stated focus on cyber security, the general recognition by all market participants that most entities are subject to some degree of material cyber security risk, and the potential for liability if material cyber security risks are not appropriately disclosed, issuers and their boards of directors would be well advised to formalize their framework for assessing the particular cyber security risks and evaluating and implementing appropriate risk mitigation strategies. This will not only assist issuers in providing timely and effective disclosure, but in developing and implementing effective strategies for mitigating cyber security risk and monitoring possible cyber security breaches.

For further information regarding cyber security risks, incidents and disclosure in Canada, please contact any member of our Corporate Securities or Technology Groups.