JANUARY 2017

CYBERSECURITY & SECURITIES AND CAPITAL MARKETS BULLETIN

Borden Ladner Gervais

Cyber Risk Management – Regulatory Guidance for Reporting Issuers' Continuous Disclosure of Cybersecurity Risks and Incidents

On January 19, 2017, the Canadian Securities Administrators (CSA) published *Multilateral Staff Notice 51-347 - Disclosure of cyber security risks and incidents* to explain CSA's expectations for continuous disclosure regarding cybersecurity risks and incidents by "reporting issuers" – companies that have issued shares to the public. The Multilateral Staff Notice supplements a previous CSA notice regarding cybersecurity risk management, and provides helpful guidance to assist reporting issuers to comply with their legal obligations to ensure that investors have timely, material information to make informed investment decisions.

Staff Notice 11-322 – Cyber Security

In September 2016, CSA published *Staff Notice 11-322 - Cyber Security* to highlight the importance of cybersecurity risks for financial market participants, outline CSA's cybersecurity initiatives to assess and promote market participant readiness and resilience, and set out general expectations for financial market participants' cybersecurity risk management activities. The 2016 Staff Notice also summarized some key cybersecurity recommendations in guidance documents issued by regulatory authorities and standard-setting bodies (e.g. Investment Industry Regulatory Organization of Canada and Mutual Fund Dealers Association of Canada). For more information, see BLG Bulletins *Cyber Risk Management – Regulatory Guidance From The Canadian Securities Administrators* and *In the wake of the Yahoo breach, the CSA offers timely guidance to public companies*.

Multilateral Staff Notice 51-347 – Disclosure of cyber security risks and incidents

CSA's *Multilateral Staff Notice 51-347* explains CSA's expectations for reporting issuers' compliance with continuous disclosure obligations as they apply to cybersecurity risks and incidents.

1. Continuous Disclosure Obligations

Canadian securities laws require every reporting issuer to make continuous disclosure of material information about the issuer's business so that investors have equal access to information that may affect their investment decisions. There are two kinds of continuous disclosure obligations – periodic disclosure and timely disclosure.

- **Periodic Disclosure:** A reporting issuer must make disclosure at regular intervals (e.g. annually and quarterly) by filing and disseminating prescribed documents (e.g. financial statements and related management discussion and analysis and management information circulars) that include all "material facts" about the issuer. A "fact" is considered "material" if it significantly affects, or would reasonably be expected to have a significant effect on, the market price or value of the issuer's securities.
- **Timely Disclosure:** A reporting issuer must make timely disclosure, by promptly issuing a press release and filing a material change report within ten days, if there has been a "material change" in the issuer's affairs. A "material change" means either: (a) a change in an issuer's business, operations or capital that would reasonably be expected to have a significant effect on the market price or value of the issuer's securities; or (b) a decision to implement that kind of change has been made by the issuer's directors or by the issuer's senior management who believe that the issuer's directors will probably confirm the change.

Materiality is the standard for determining whether information must be disclosed. A "change" or "fact" regarding an issuer is considered "material" if it would reasonably be expected to have a significant effect on the market price or value of any of the issuer's securities. There is no bright line test for materiality. Rather, it is a question of mixed fact and law based on the specific facts and the issuer's particular circumstances.

A reporting issuer's failure to comply with continuous disclosure obligations can have serious consequences for the issuer and its directors and officers, including quasi-criminal, administrative or civil proceedings (including class action proceedings) resulting in various sanctions (e.g. a temporary or permanent cease trade order, delisting from the applicable stock exchange, disgorgement of profits and liability for damages).

2. Disclosure of Cybersecurity Risks and Incidents

(a) Cybersecurity Risks

The Multilateral Staff Notice provides guidance regarding reporting issuers' disclosure of cybersecurity risks, which we summarize as follows:

- **Materiality:** A reporting issuer's disclosure should focus on cybersecurity risks that are "material" based on the ways in which the issuer is exposed to cybersecurity risks and the kinds of cybersecurity incidents to which the issuer is likely to be exposed. Materiality should be determined by assessing the probability that a cybersecurity incident will occur and the anticipated magnitude of the incident. A cybersecurity risk that is material to one reporting issuer is not necessarily material to another issuer.
- **Specific/Detailed Disclosure:** A reporting issuer's disclosure about material cybersecurity risks should be as detailed and entity specific as possible, tailored to the issuer's specific circumstances and avoid boilerplate language, so that investors are able to understand the issuer's level of exposure to, and preparedness for, cybersecurity risks and how cybersecurity risks might impact the issuer. A reporting issuer should disclose specific risks, not merely generic risks common to all issuers. A reporting issuer is not expected to disclose information that is sensitive or that could compromise the issuer's cybersecurity.
- **Considerations:** In assessing disclosure obligations, a reporting issuer should consider the factors identified by the International Organization of Securities Commissions (IOSCO) in its April 2016 report titled *Cyber Security in Securities Markets – An International Perspective*, including: the reasons the issuer might be exposed to a cybersecurity incident, the source and nature of the risks of cybersecurity breaches, the potential consequences of a cybersecurity breach, the adequacy of the issuer's preventative measures, the issuer's prior material cybersecurity incidents and their effects on the issuer's cybersecurity risk. The IOSCO report provides additional helpful information regarding cybersecurity risk disclosure, and explains that an issuer's cybersecurity risk disclosure should include three main kinds of information: (a) descriptions of material cybersecurity risks; (b) the likely outcomes of a cybersecurity incident; and (c) how the issuer is managing cybersecurity risks.
- **Mitigation and Governance:** A reporting issuer should disclose how it mitigates the risk of cybersecurity incidents, including whether and to what extent the issuer maintains insurance for cybersecurity incidents and the issuer's reliance on third party experts for the issuer's cybersecurity strategy or to remediate cyber incidents. A reporting issuer should also disclose information about the issuer's cybersecurity risk governance, including identifying the committee or person responsible for the issuer's cybersecurity and risk mitigation strategy.
- **Controls:** A reporting issuer's disclosure controls and procedures should be applied to ensure that detected cybersecurity incidents are communicated to the issuer's management for timely disclosure decisions.

(b) Cybersecurity Incidents

The Multilateral Staff Notice also provides guidance regarding reporting issuers' timely disclosure of cybersecurity incidents, which we summarize as follows:

- **Independent Obligation:** Securities legislation obligations to timely disclose cybersecurity incidents are different from reporting or notification obligations under privacy laws or other legislation.
- **Materiality:** Whether and when a reporting issuer must disclose a cybersecurity incident will depend on whether the incident is a "material fact" or a "material change" that requires disclosure under securities laws. The materiality of a cybersecurity incident and the kinds of disclosures required must be determined based on a contextual analysis of the incident and related circumstances, including the impact of the incident on the issuer's operations and reputation, customers, employees and investors. There is no bright-line test for materiality, and the quantitative or qualitative threshold for materiality will vary depending on the circumstances. The determination of whether a cybersecurity incident is material is a dynamic process throughout the different phases (e.g. detection, assessment and remediation) of the incident response process.
- **Planning:** A reporting issuer's cybersecurity incident response plan should address how the materiality of a cybersecurity incident will be assessed to determine whether and what, and when and how, to disclose the incident.
- **Disclosure:** If a reporting issuer has determined that a cybersecurity incident should be disclosed, then it might be appropriate to disclose information regarding the anticipated impact and costs of the incident.

Comment

In addition to continuous disclosure obligations under securities laws, a reporting issuer might be subject to cyber incident notification obligations imposed by statute (e.g. personal information protection laws), contract (e.g. confidentiality or data security obligations) or generally applicable common law or civil law (e.g. duty to warn). All of those obligations should be considered by a reporting issuer when determining whether, when and how to disclose a cybersecurity incident.

To comply with continuous disclosure obligations regarding cybersecurity risks, a reporting issuer will have to establish the kind of risk identification and assessment processes that are an essential component of an effective cybersecurity risk management program. Regulators, industry associations and other organizations have emphasized that all kinds of organizations (not just reporting issuers) should have a documented, comprehensive cybersecurity risk management program, and have provided useful guidance and tools for the assessment and mitigation of cybersecurity risks.

A comprehensive program for cybersecurity risk identification and assessment is also necessary for corporate directors and officers to fulfil their duties of care regarding cybersecurity risk management. Regulators, industry associations and other organizations have emphasized that corporate directors must be engaged and take an active role in their corporations' cybersecurity risk management activities, and must ensure that their corporations have appropriate policies and procedures in place to manage cybersecurity risks in the context of their businesses and to effectively respond to cybersecurity incidents.

For more information, see BLG Bulletins *Cyber-Risk Management – Data Incident Notification Obligations*, *Cybersecurity Guidance From Investment Industry Organization*, *Cybersecurity Guidance From Investment Industry Organization*, *U.S. Securities and Exchange Commission Issues Cybersecurity Guidance Update*, *Cyber-Risk Management Guidance From Financial Institution Regulators*, *Regulatory Guidance for Cyber Risk Self-Assessment*, and *Cyber-Risk Management – Guidance For Corporate Directors*. ■

Authors

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

Joseph DiPonio
T 416.367.6292
jdiponio@blg.com

For more information about Cybersecurity and BLG's related legal services, please **click here**.

For more information about Securities and Capital Markets and BLG's related legal services, please **click here**.

Borden Ladner Gervais

BORDEN LADNER GERVAIS LLP
LAWYERS | PATENT & TRADEMARK AGENTS

Calgary
Centennial Place, East Tower
1900, 520 – 3rd Ave S W, Calgary, AB, Canada T2P 0R3
T 403.232.9500 | F 403.266.1395

Montréal
1000 De La Gauchetière St W, Suite 900
Montréal, QC, Canada H3B 5H4
T 514.879.1212 | F 514.954.1905

Ottawa
World Exchange Plaza, 100 Queen St, Suite 1300
Ottawa, ON, Canada K1P 1J9
T 613.237.5160 | F 613.230.8842 (Legal)
F 613.787.3558 (IP) | ipinfo@blg.com (IP)

Toronto
Bay Adelaide Centre, East Tower
22 Adelaide St W, Suite 3400, Toronto, ON, Canada M5H 4E3
T 416.367.6000 | F 416.367.6749

Vancouver
1200 Waterfront Centre, 200 Burrard St, P.O. Box 48600
Vancouver, BC, Canada V7X 1T2
T 604.687.5744 | F 604.687.1415

blg.com