CPA CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

Reporting Alert

CORPORATE REPORTING

APRIL 2017

Cyber Security Risks and Incidents—Reassessing Your Disclosure Practices

In today's fast-paced, highly connected business environment, various aspects of an organization's business activities are carried out in "cyberspace". Cyberspace is where people and organizations create an electronic presence and engage in virtual activities, exchanging information, products and services through the Internet.[1] While operating in cyberspace offers advantages, it also makes organizations vulnerable to cyber attacks by criminals with far-reaching consequences beyond the theft of information and financial losses.[2]

Cyber security is a response to cyberspace risks and refers broadly to the processes and practices in place to protect computer systems and data from threats originating in cyberspace. Given the significant reputational, operational, financial, legal, and regulatory implications of recent high-profile data breaches, investors are increasingly interested in understanding an organization's exposure to cyber security risk and the related policies, processes, and the controls in place to address this risk.

1 ***Board Bulletin: Cybersecurity Risk—Questions for Directors to Ask***.

2 Cyber attacks are defined in a report by the board of the International Organization of Securities Commissions (IOSCO) as "attempts to compromise the confidentiality, integrity and availability of computer data or systems." ***Cyber Security in Securities Markets—An International Perspective, April 2016***.

Significant judgment must be exercised in determining whether cyber security risks and incidents are material and require disclosure under existing disclosure obligations. By nature, cyberspace risks are very complicated and the nature and extent of disclosure about cyber security risk exposure in practice will vary greatly from one entity to another depending on its unique circumstances. There are many areas where existing disclosure obligations may require companies to disclose information about cyber security risks. For example:

- **Annual Information Form (AIF):** A reporting issuer must disclose risk factors, including the general risks inherent in the nature of the company's business, and any other matter that would be most likely to influence an investor's decision to purchase securities of the company.
- **Management's Discussion and Analysis (MD&A):** MD&A requirements include a discussion of, among other things, important trends and risks that have already affected the financial statements, and trends and risks that are reasonably likely to affect them in the future.
- **Material Change Report:** When a material change occurs in the affairs of a reporting issuer, the issuer must immediately issue and file a news release disclosing the nature and substance of the change, and must also file a Material Change Report as soon as practicable within 10 days of the change.
- **Financial Statements:** Cyber security risks and incidents may also affect financial statement disclosures (e.g., costs and other consequences associated with material cyber incidents).

In addition to reporting information required to comply with securities regulations, many issuers seek to identify and address other matters of interest to their stakeholders (e.g., in supplementary documents available on their websites).

CSA Staff Notice 51-347

On January 19, 2017, the Canadian Securities Administrators (CSA) published **CSA Multilateral Staff Notice 51-347 Disclosure of cyber security risks and incidents** (CSA Staff Notice 51-347 or Staff Notice) which outlined expectations for disclosures by reporting issuers relating to cyber security risks and cyber incidents.

This *Reporting Alert* provides an update on CSA Staff Notice 51-347 and issues relating to cyber security disclosure. It does not address the underlying cyber security practices and procedures and does not attempt to provide advice on how to comply with securities regulations. Whether disclosure in documents filed under securities regulations comply with applicable requirements is ultimately a legal matter and should be considered carefully. The information included in this *Reporting Alert* is for general information purposes only and should not be used as a substitute for reviewing CSA Staff Notice 51-347 and consultation with professional advisors.

Main Findings

The Staff Notice is based on a review of disclosure around cyber security risks and cyber incidents. The review was informed in part by the report, ***Cyber Security in Securities Markets—An International Perspective***, issued by the board of the International Organization of Securities Commissions (IOSCO) in April 2016 (IOSCO report). CSA staff reviewed the securities filings of the 240 constituents of the S&P/TSX Composite Index and focused on:

- whether and how issuers had addressed cyber security issues in their risk factor disclosure, including whether the disclosure described potential impacts of a cyber attack on the issuer's business
- what kind of material information could be exposed as a result
- who was responsible for the issuer's cyber security strategy
- disclosure about any previous cyber security incidents.

Disclosure of Cyber Security Risk

CSA Staff found that 61% of the issuers they reviewed addressed cyber security issues in their risk factor disclosure, acknowledging that their dependence on information technology systems rendered them at risk for cyber security breaches. However, fewer issuers provided disclosure regarding their *particular* vulnerability to cyber security incidents arising, for instance, from the industry in which they operate, their ownership of specified assets, the nature of their operations, their status as government contractors, or the nature of their information technology systems. Some issuers addressed the risk that third parties could expose them to cyber security issues.

Disclosure of Potential Impacts of a Cyber Security Incident

Issuers that addressed cyber security issues in their risk factor disclosure went on to specify that disruptions due to cyber security incidents could adversely affect their business, results of operations and financial condition. Potential impacts cited by issuers across different industries included:

- compromising of confidential customer or employee information
- unauthorized access to proprietary or sensitive information
- destruction or corruption of data
- lost revenue due to a disruption of activities
- reputational harm affecting customer and investor confidence
- diminished competitive advantage and negative impacts on future opportunities
- effectiveness of internal control over financial reporting.

Some industry and business-specific potential impacts identified by issuers included:

- operational delays (e.g., production downtimes or plant and utility outages)
- inability to manage the supply chain
- inability to process customer transactions or to otherwise service customers
- disruptions to inventory management
- loss of data from research and development activities
- devaluation of intellectual property.

Disclosure of Governance and Cyber Security Risk Mitigation

CSA staff found that 20% of the issuers addressing cyber security in their disclosure identified a person, group or committee as being responsible for overseeing their cyber security risks. These issuers most often identified the audit committee as holding this responsibility, often in discussion with management.

Other issuers cited a risk committee, the board of directors and management as a whole, or individuals such as the chief financial officer or the head of information technology. Some issuers addressed their disaster recovery plan or their controls in place over unauthorized access. However, few issuers addressed the adequacy or inadequacy of insurance coverage against such incidents.

CSA Staff Guidance

General

The Staff Notice suggests disclosure should focus on material and entity-specific information. Boilerplate language should be avoided; entity-specific language should enable the reader to distinguish one issuer from another within the same industry or across industries with regard to the level of exposure, the level of preparedness and how the risk impacts the issuer. Materiality assessments are informed by an analysis of the probability that a breach will occur and the anticipated magnitude of its effect. CSA Staff do not expect issuers to disclose details regarding their cyber security strategy or their vulnerability to cyber attacks that are of a sensitive nature or that could compromise their cyber security.

Risk and Exposure

Appropriate disclosures might address the reasons why an issuer may be exposed to a cyber security breach, the source and nature of the risks, the potential consequences of a breach, and the adequacy of preventative measures. The disclosure might also encompass prior material cyber security incidents and their effects on the issuer's cyber security risk.

Mitigation

Issuers should address how they mitigate cyber security risk, including their degree of reliance on third-party experts for their cyber security strategy or to remediate prior or future cyber attacks. Issuers should also look at governance issues, including identifying a committee or person responsible for the issuer's cyber security and risk mitigation strategy. The disclosure might also examine the nature and extent of relevant insurance coverage. The Staff Notice cites the IOSCO report as an important reference in assessing the adequacy of disclosure.

Timely Disclosure

After a cyber security incident takes place, the issuer must determine whether it is a material fact or material change that requires disclosure in accordance with securities legislation. Again, no bright-line test exists for this assessment; the threshold at which a cyber security breach becomes material may vary among issuers and industries. The Staff Notice acknowledges that the consequences of a cyber security incident (and therefore its materiality) may take time to assess fully. While an isolated cyber attack may not be material, repeated or frequent minor incidents may become material in light of the level and type of disruption caused.

In any plan for response following a cyber attack, CSA Staff expects issuers to address how they would assess the materiality of the attack in order to determine whether, what, when and how to disclose externally.

Some Questions for Management and Boards

The following key questions may assist management and boards of reporting issuers when assessing their cyber risk disclosure practices:

1. Have we documented and do we fully understand the cyberspace in which we and our business partners operate?
2. Have we assessed the overall adequacy of our disclosure of cyber security risk with reference to the considerations set out in the CSA Staff Notice?
3. Have we assessed separately, for each of our core periodic disclosure documents, what disclosure is required about cyber security risk from an operational, financial and regulatory perspective? Do we have procedures in place to revisit this disclosure regularly?
4. Have we defined internal procedures for assessing the materiality of cyber security breaches or other occurrences?
5. Have we assessed cyber security risk disclosures made by other companies in our industry or in similar circumstances?
6. Have we taken steps to understand what concerns our investors may have about our exposure to cyber security risk, and how we should address these concerns in our disclosure?
7. Does the design of our disclosure controls and procedures include processes to ensure cyber security incidents are communicated to management, and that consequent disclosure decisions are made in a timely manner?
8. Do we understand how our external auditors take cyber security risk into account when planning and performing their audit?

9. Are we satisfied that cyber security risk and its mitigation receive appropriate attention in our governance structure? Is it clear where the responsibility lies for overseeing this area?

   Does the individual or group responsible for overseeing cyber security risk devote sufficient time to these issues, and receive appropriate input, support and resources from our organization as a whole? Is all of this sufficiently clear in our disclosures?

10. Have we developed internal key performance measures relating to how we monitor, detect and manage cyber security risk? If so, should we disclose these in our external reporting?

Other Resources:

- *CSA Staff Notice 11-326 Cyber Security*
- *CSA Staff Notice 11-332 Cyber Security*
- *Board Bulletin: Cybersecurity Risk—Questions for Directors to Ask*

Comments on this *Reporting Alert*, or suggestions for future Reporting Alerts should be sent to:

Rosemary McGuire, CPA, CA
Principal, Reporting & Capital Markets
Research, Guidance and Support
Chartered Professional Accountants of Canada
277 Wellington Street West
Toronto ON M5V 3H2
Email: rmcguire@cpacanada.ca