CSA/ACVM Canadian Securities Administrators Autorités canadiennes en valeurs mobilières

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

January 19, 2017

Introduction

Cyber security was identified as a priority area in the CSA 2016-2019 Business Plan. On September 27, 2016, the Canadian Securities Administrators (the **CSA**) published Staff Notice 11-332 *Cyber Security* (**Staff Notice 11-332**) in order to highlight the importance of cyber security risks for issuers, registrants and regulated entities and inform stakeholders about recent and upcoming CSA initiatives. With respect to issuers, Staff Notice 11-332 indicated that CSA members would examine the disclosure of some of the larger issuers to analyze what is being disclosed with respect to cyber security risk and cyber attacks.

Accordingly, CSA Staff recently reviewed the disclosure provided by the constituents of the S&P/TSX Composite Index regarding cyber security risk and cyber attacks. Staff from the British Columbia Securities Commission, the Ontario Securities Commission and the Autorité des marchés financiers (**staff** or **we**) are publishing this notice (the **Staff Notice**) to report the findings of our review and provide disclosure expectations for reporting issuers.

Staff in certain CSA jurisdictions have carried out cyber security disclosure reviews in the past, including as part of their work on the International Organization of Securities Commissions (**IOSCO**) report on cyber security in securities markets (the **IOSCO Report**).[1] This Staff Notice, however, presents the results of a review of issuers that is larger in scope. The review was undertaken as we are of the view that issuers in all industries may be exposed to cyber security risk, albeit in different ways.

Issue-oriented review

We reviewed the most recent annual filings of the 240 constituents of the S&P/TSX Composite Index[2], including issuers' annual information forms, management's discussion and analysis, management information circulars, as well as other filings such as material change reports and news releases.

The review 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, and who

[1] IOSCO report on cyber security in securities markets
http://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf
[2] As at July 7, 2016.

was responsible for the issuer's cyber security strategy. We also searched for disclosure about any previous cyber security incidents.

Risk factor disclosure

Disclosure of cyber security risk

In our review, we found that 146 of the 240 issuers, or 61%, addressed cyber security issues in their risk factor disclosure.

Issuers generally disclosed that their dependence on information technology systems renders them at risk for cyber security breaches. We note that issuers in a wide variety of industries acknowledged cyber security as a material risk to their business.

We also note that few issuers provided disclosure regarding their particular vulnerability to cyber security incidents. For example, some of those issuers identified the industry in which they operate, their ownership of specified assets, the nature of their operations or their status as government contractors, as factors increasing the likelihood that they could be targets of cyber surveillance or a cyber attack from cyber criminals, industrial competitors or government actors. Others disclosed that their information technology systems were based on legacy technology and operated with a minimal level of available support.

Some issuers also addressed the risk that third parties could expose them to cyber security issues. Third party security breaches, the inadequate levels of cyber security expertise and safeguards of third party partners, and the failure or ending of third party information technology services on which the issuer relies are among those risks.

Disclosure of potential impacts of a cyber security incident

Issuers that recognized the dependence of their business operations on information technology systems disclosed that disruptions due to cyber security incidents could adversely affect their business, results of operation and financial condition.

The following frequently identified potential impacts of a cyber security incident were common to a variety of issuers across different 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;

- effectiveness of internal control over financial reporting.

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

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

Disclosure of governance and cyber security risk mitigation

We examined whether and whom issuers identified as being responsible for their cyber security strategy. We found that 31 issuers, or 20% of the issuers who had addressed cyber security in their disclosure, had identified a person, group or committee.

The audit committee was most often identified as being responsible for overseeing the issuer's cyber security risks, often in discussion with management. Some issuers indicated that a risk committee was responsible for overseeing and managing risks such as cyber security. The board of directors and management as a whole were also identified, while a few issuers identified the Chief Financial Officer or the head of information technology as being responsible for overseeing cyber security risks.

Some issuers disclosed that controls such as a disaster recovery plan and controls over unauthorized access have been put in place. Few issuers disclosed holding insurance against cyber security incidents, while some issuers also noted that they may be insufficiently covered for such incidents.

Staff guidance on risk factor disclosure

As a general principle, disclosure should focus on material and entity specific information, and avoid boilerplate language. While we acknowledge that exposure to cyber security risks may be common to all issuers in every industry, issuers should bear in mind that one of the purposes of risk factor disclosure is to allow the reader to distinguish one issuer from another, within the same industry or across industries, in terms of the level of exposure, the level of preparedness and how the risk impacts the issuer.

As issuers are increasingly dependent on information technology to operate their business, and as cyber attacks are becoming more frequent and sophisticated, we expect that issuers will consider the ways in which, as well as the types of cyber attacks to which, they are likely to be exposed.

We recognize that all issuers may be exposed to a cyber attack. However, issuers in different industries may be subject to cyber security risk for reasons different than issuers in other industries, and may be exposed to varying degrees. For example, the vulnerability of a consumer-facing issuer is different than that of an issuer owning strategic intellectual property or

operating infrastructure assets. The consequences of a cyber attack may also differ greatly between issuers.

As discussed in Staff Notice 11-332, CSA members expect issuers, to the extent that they have determined that cyber security risk is a material risk, to provide risk disclosure that is as detailed and entity specific as possible. Materiality in cases of a cyber security risk turns on an analysis of the probability that a breach will occur, and the anticipated magnitude of its effect.

Given that we expect issuers to disclose specific risks rather than generic risks common to all issuers, we expect issuers to tailor their disclosure of cyber security risk to their particular circumstances. However, we do 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.

We expect issuers to consider the factors identified by IOSCO when preparing their disclosure. Issuers should consider the reasons they may be exposed to a cyber security breach, the source and nature of the risks, the potential consequences of a cyber security breach, the adequacy of preventative measures, as well as a consideration of prior material cyber security incidents and their effects on the issuer's cyber security risk. Issuers should also address how they mitigate the risk, including whether and to what extent the issuer maintains insurance covering cyber attacks, or reliance on third party experts for their cyber security strategy or to remediate prior or future cyber attacks. It is also relevant to disclose governance issues, including identifying a committee or person responsible for the issuer's cyber security and risk mitigation strategy. We refer issuers to Chapter 2 of the IOSCO Report.

Finally, we expect that 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* apply such disclosure controls and procedures to detected cyber security incidents, in order to ensure these incidents are communicated to management and a decision regarding whether and what to report is made in a timely manner.

Cyber security incident disclosure

Although a few issuers addressed in their risk factor disclosure that they had been subject to cyber attacks in the past, no issuers in our sample disclosed such incidents as being material. Only one issuer in our sample had issued a press release following a data breach resulting in confidential information being accessed and disclosed; however, the issuer did not file a material change report in connection with this incident.

We note that certain issuers have disclosed in their continuous disclosure filings that they have been subject to cyber security breaches in the past, but that these incidents were not material.

Staff guidance on incident reporting

We understand that privacy or other legislation may require issuers to report or notify persons of cyber security breaches in certain circumstances, but such obligations are different than those provided by securities legislation.

In considering whether and when to disclose a cyber security incident, the issuer must determine whether it is a material fact or material change that requires disclosure in accordance with securities legislation. The issuer should refer to the guidance in National Policy 51-201 *Disclosure Standards* and may in addition refer to the provisions of Part 1(f) of Form 51-102F1 *Management's Discussion & Analysis* and Part 1(e) of Form 51-102F2 *Annual Information Form* of National Instrument 51-102 *Continuous Disclosure Obligations*.

We recognize that there is no bright-line test and that the quantitative or qualitative threshold at which a cyber security breach becomes material may vary between issuers and industries, depending on the circumstances of the issuer as well as on the type of incident and the extent of the consequences.

Materiality depends on the contextual analysis of the cyber security incident. While an isolated cyber attack may not be material, a series of or frequent minor incidents may become material in light of the level and type of disruption caused. The impact of a distributed denial-of-service attack or ransomware would differ from that of a cyber security breach aimed at obtaining client information. The types of disclosure required, whether in the issuer's risk factor disclosure, financial reporting or incident reporting, depends on the circumstances of the incident.

Timing is an important factor in reporting material cyber security incidents. We understand that cyber security incidents may not be detected until much later than when they occurred, and the consequences of the incident may take time to fully assess. The determination of whether the incident is material is a dynamic process throughout the detection, assessment and remediation phases of a cyber security incident.

As indicated in Staff Notice 11-332, we expect issuers to address in any cyber attack remediation plan how materiality of an attack would be assessed to determine whether and what, as well as when and how, to disclose in the event of an attack. In the assessment, issuers should consider the impact on the company's operations and reputation, its customers, employees and investors. Where an issuer has determined a cyber security incident should be disclosed, it might be appropriate to consider and provide visibility as to the anticipated impact and costs of the incident.

Next Steps

Staff intends to continue reviewing disclosure of cyber security risks and incidents, monitor trends in disclosure and review the extent and timing of reporting of cyber security incidents.

Questions

Please refer your questions to any of the following:

Georgia Koutrikas
Analyst, Corporate Finance
Autorité des marchés financiers
514-395-0337 ext: 4393
georgia.koutrikas@lautorite.qc.ca

Martin Latulippe
Director, Continuous Disclosure
Autorité des marchés financiers
514-395-0337 ext: 4331
martin.latulippe@lautorite.qc.ca

Matthew Au
Senior Accountant, Corporate Finance Branch
Ontario Securities Commission
416-593-8132
mau@osc.gov.on.ca

Allan Lim
Manager, Corporate Finance
British Columbia Securities Commission
604-899-6780
alim@bcsc.bc.ca