CSA PUBLISH UPDATE ON CYBERSECURITY FOR MARKET PARTICIPANTS

Posted on October 6, 2016

Categories: Insights, Publications

Today's issuers, registrants, and regulated entities (collectively, Market Participants) rely increasingly on electronic systems to, among other things, store confidential information, transfer data and intellectual property, record transactions, and track key financial assets. As such, these systems are attractive targets for threat agents seeking to compromise the confidentiality, integrity, reliability or availability of Market Participants' information or their operational capability.

Recent studies suggest an upswing in the frequency and complexity of cyber attacks. Detection of security incidents in 2015 had increased by 38% over the year prior. Cyber attacks are also becoming more costly: a 2016 Ponemon Institute study of 383 companies across 16 industries in 12 countries revealed that the average total cost of a data breach per company was US$4 million, up from US$3.79 million last year.

On September 27, 2016, the Canadian Securities Administrators (CSA) published CSA Staff Notice 11-332 *Cyber Security* (the 2016 Notice), noting these trends and proposing cybersecurity related policy initiatives to help Market Participants reduce their exposure to cyber risk. The Notice updates CSA Staff Notice 11-326 *Cyber Security* (the 2013 Notice), which was discussed in our October 2013 bulletin. Briefly, the 2013 Notice reminded Market Participants to take appropriate protective measures to safeguard themselves, their clients, and stakeholders against cyber risk, follow guidance and best practices from industry groups, and regularly review cyber risk control measures.

The 2016 Notice elaborates on these points and provides enhanced and updated guidance to Market Participants based on developments in the cybersecurity landscape since 2013. In its 2016-2019 Business Plan, the CSA set the following priorities under the larger objective of enhancing cybersecurity:

- Improve collaboration and communication on cybersecurity issues with Market Participants, including reporting issuers, registrants and other regulated entities;
- Assess the level of Market Participant cybersecurity resilience, including measures for protection of personal investor data; and

- Improve Market Participants' understanding of CSA members' cybersecurity oversight activities, including providing guidance on expectations for Market Participants' cybersecurity preparedness.

In line with the priorities discussed in its business plan, the 2016 Notice reminds Market Participants of the following:

I. Issuers

Once an issuer has determined that cyber risk is a material risk, it should provide detailed and entity-specific risk disclosure and avoid general, boilerplate disclosure. Any cyber attack remediation plan should address how the issuer would assess the materiality of a cyber attack to determine what needs to be disclosed pursuant to applicable securities laws, as well as when and how.

Over the coming months, CSA members intend to re-examine the disclosure of some larger issuers to better understand how they assess materiality with respect to cyber risk. The CSA intends to publish any findings or recommendations stemming from those reviews shortly thereafter.

II. Registrants

Registrants must remain vigilant in developing, implementing, and updating their approach to cybersecurity "hygiene and management". The CSA urges registrants to review and follow guidance issued by self-regulatory organizations such as the Investment Industry Regulatory Organization of Canada and the Mutual Fund Dealers Association of Canada.

Some CSA members are in the process of gathering data about registrants' cybersecurity practices. The CSA anticipates that a targeted desk review will be planned for later this year, which will assess in more detail areas discussed in regular compliance reviews.

III. Regulated Entities

Marketplaces, clearing agencies, information processors and trade repositories that operate in Canada must perform independent system review, which includes a specific focus on cybersecurity. The CSA expects regulated entities to adopt a cybersecurity framework provided by a regulatory authority or standard-setting body appropriate to their size and scale and, in the 2016 Notice, the CSA notes that it has been gathering information to better understand how regulated entities are positioned with respect to such adoption.

Regulated entities should examine and review their compliance with ongoing requirements outlined in securities legislation, which include the need to have internal controls over their systems and to report security breaches.

What's Next?

The CSA notes that it has engaged with international initiatives related to cyber risk and resilience, such as those undertaken by entities like the International Organization of Securities Commissions. These initiatives include developing cyber resilience frameworks, publishing reports on regulatory approaches and tools aimed at managing cyber risk and enhancing cross-border cybersecurity information sharing among regulators.

The CSA plans to hold roundtable sessions in the coming months to discuss cybersecurity issues and risks, regulatory expectations, the need for collaboration and communication on issues relating to cybersecurity and the need for coordination in the event of a cyber incident.

The CSA expects Market Participants to actively protect themselves against cyber threats, and in the 2016 Notice references a number of documents and resources that Market Participants may find useful in this pursuit. While stressing that each organization should establish cybersecurity frameworks tailored to their particular circumstances, the CSA recommends that Market Participants ensure that personnel at all levels, including management, be responsible for cybersecurity, establish robust cybersecurity policies and frameworks (which, among other things, address how to mitigate the damage of the breach and any reporting obligations flowing therefrom) and improve communication and collaboration with other interested parties.

by Arman G. Farahani, Rohan Hill and Bill Olaguera, Articled Student

A Cautionary Note