CSA PROVIDES GUIDANCE TO REGISTRANTS ON CYBER SECURITY AND SOCIAL MEDIA

Posted on November 1, 2017

Categories: Insights, Publications

Following the ongoing rise of cyber security breaches, the Canadian Securities Administrators (the "**CSA**") regulatory authorities continue to heighten expectations with respect to cyber security policies of registered firms. On October 19, 2017, the CSA released Staff Notice 33-321 *Cyber Security and Social Media* (the "**Staff Notice**"). The Staff Notice summarizes the results of a survey of 1,000 registered firms with a 63% response rate, which examined cyber security and social media practices over the period from October 11, 2017 to November 4, 2016 (the "**CSA Survey**").

The CSA Survey found that more than half of the registered firms surveyed (51%) had experienced a cyber security incident. The most common incident was phishing (43%), followed by malware issues (18%) and fraudulent emails impersonating clients (15%).

The CSA Survey collected data on seven aspects of cyber security practices: (i) policies and procedures, (ii) training, (iii) risk assessments, (iv) incident response plans, (v) due diligence, (vi) data protection and (vii) insurance.

Cyber Security

Policies and Procedures

The CSA Survey found that while most registered firms have some form of cyber security policy, only 57% of firm cyber security policies address continued operation of the registered firm during a cyber security incident. Furthermore, the CSA Survey noted that only 56% of the registered firms have policies and procedures for training employees on cyber security.

The CSA recommended that cyber security policies of registered firms should, among other things, address the following areas of risk:

- electronic communications,
- the use of firm issued electronic devices,
- the loss or disposal of an electronic device,

- use of public electronic devices or public internet connections,
- detecting internal or external unauthorized activity on the firms network,
- ensuring up-to-date software and anti-virus programs,
- oversight of third party vendors, and
- reporting any cyber security incidents to the firm's board of directors (or equivalent).

Training

The CSA Survey found that employee cyber security training tends to focus on suspicious emails, developing good passwords and use of hardware or software. However, the CSA recommended that registered firms should also include training in areas such as handling confidential information, device security, procedures for reporting incidents and the types of threats that may be encountered. It is also important for registered firms to ensure that they provide training with sufficient frequency to remain current with cyber security developments.

Risk Assessments

The CSA Survey found that while most firms perform risk assessments at least annually, although 14% of firms do not conduct such assessments at all.

The CSA recommended that risk assessments should be conducted at least annually and should take the following into account:

- the firm's critical assets and confidential information,
- areas of operational vulnerability,
- how threats can be identified,
- consequences of threats to the firm, and
- adequacy of the firm's prevention and response plans.

Incident Response Plan

The CSA Survey found that 66% of firms test their cyber security response plan at least annually. The CSA recommended that firms should have a written response plan to address cyber security incidents, which should include the following:

- designate personnel responsible for incident reporting and response,
- describe the types of threats the firm may face,
- outline procedures to end the attack and for data recovery,
- identify any parties that must be notified, and

- include an investigation of the extent of any damage.

Due Diligence

The CSA also recommended that registered firms should limit third-party access of its systems and data and ensure that written agreements with such vendors include: (i) notice requirements for any cyber security incident and (ii) an adequate response plan from the third parties.

Data Protection

The CSA Survey found that a sizable number of registered firms do not use any encryption when storing and accessing client data through various technologies such as email, cloud storage and websites. All but four registered firms that responded to the survey backed up data on a periodic basis and 89% of firms have tested their backup recovery process.

The CSA recommended that firms should encrypt data for all computers and devices and all devices should be password protected. Passwords should contain different types of characters and should be frequently changed. Further, the CSA expects firms to back up their data off-site to a secure server and regularly test their back-up process.

Insurance

A majority of firms (59%) do not have cyber-security-specific insurance policies. The CSA recommends that firms should confirm whether their existing insurance policies provide any coverage for cyber security incidents, and if not, firms should consider expanding the scope of their coverage to include such events.

Social Media

The Staff Notice also contained CSA Survey results on two aspects of social media use: (i) policies and procedures and (ii) monitoring of social media activity. It is important to note that firms may be vulnerable to cyber security attacks through social media (e.g., cyber attackers may use social media sites to launch targeted phishing e-mails or social media sites may lead to websites that install malware).

Policies and Procedures

The CSA Survey found that, while 59% of firms have guidelines on social media use, only 36% have policies and procedures for training employees about social media use and only 21% have specific recordkeeping policies for communications via social media.

The CSA recommends that firms define appropriate social media use and content, ensure that information on social media is current, keep records of social media content, and implement an approval and monitoring

process for social media content.

Monitoring of Social Media Activity

The CSA Survey found that only 14% of firms engage in real-time monitoring of social media activity and 6% of firms do not monitor social media activity at all. Of the firms that monitor the use of social media by employees for business purposes, 46% conduct spot checking or a sample review.

The CSA recommended that, given the ease with which information may be posted on social media platforms and the difficulty of removing the information thereafter, registered firms should monitor social media use in a timely manner and have appropriate approval procedures for social media communications. Even if registered firms prohibit social media use for business purposes, policies and procedures should be in place to monitor unauthorized use.

Overall, the CSA's study demonstrates that registered firms are considering the risks associated with cyber security and social media, and have begun to implement measures to address such risks. However, the CSA's guidance on this issue suggests that there are some registered firms that should do more to reduce their cyber security and social media risks going forward.

by Jeffrey Nagashima, Valenteena Suvaminathan and Anthony Pallotta, Student-at-Law

A Cautionary Note