CSA Publishes Guidance on Cyber Security and Social Media Practices of Registered Firms After Its Review of Their Current Practices

November 01, 2017
Vanessa Coiteux, Jérémie Ste-Marie

In 2017, we have witnessed increased scrutiny from the Canadian Securities Administrators (the CSA) on the subject of cyber security, with the CSA releasing a number of publications on the matter to date. More recently, on October 19, 2017, results of the CSA's survey of 630 registered firms' cyber security and social media practices were published in CSA Staff Notice 33-321 Cyber Security and Social Media (the Staff Notice). In addition to providing a picture of current practices in this area, the Staff Notice also includes guidance suggesting policies and procedures to be applied to cyber security and social media practices and reminds registered firms that they should adopt cyber security and social media practices that include preventative measures, training for all staff and a response plan for when a cyber security incident occurs.

Background

The CSA's survey was conducted in light of the growing risks posed to registered firms by cyber threats and social media. The CSA indicate that the requirement under National Instrument 31-103 *Registration Requirements, Exemptions and Ongoing Registrant Obligations* (NI 31-103) that a registrant implement a system of controls and supervision to ensure compliance with securities legislation and manage the risks associated with its business applies to the risks of cyber threats and the use of social media, both of which, according to the CSA, pose risks for all registered firms.

In CSA Staff Notice 11-332 Cyber Security, published in October 2016 and previously discussed here, the CSA stressed the need to address cyber security risks and the expectation that registered firms develop, implement and update measures to safeguard themselves and their clients from cyber threats. In addition, in CSA Staff Notice 31-325 Marketing Practices of Portfolio Managers, previously discussed here, the CSA outlined the challenges that registered firms face when using social media as a means of communication, including that social media platforms make it difficult to retain adequate business activity and client communication records as required by NI 31-103. The use of social media may also provide entry points for hackers into a firm's systems.

Results

The results published in the Staff Notice highlight, among other things, the following:

- **Cyber Security Attacks.** In 2016, approximately 51% of firms surveyed experienced a cyber security incident.

- **Cyber Security Policies and Procedures.** Only 57% of firms surveyed have specific policies and procedures to address the firm's continued operation during a cyber security incident and only 56% have policies and procedures for the training of employees about cyber security.
- **Training**. Firms provide training to employees with a focus on suspicious emails or links (70%), good password practices (68%) and safe use of hardware or software (60%). Other aspects of training programs included education about hacking attacks (59%) and downloading or installing software or applications (58%). 18% of firms did not provide cyber security specific training to employees.
- **Risk Assessments.** All but 14% of firms conduct risk assessments to identify cyber threats at least annually, if not more frequently.
- **Incident Response Plan.** The majority of firms which have a cyber security incident response plan test it at least annually. However, 25% of firms have not yet tested their incident response plan.
- **Due Diligence.** A significant number of firms surveyed (92%) have engaged third-party vendors, consultants, or other service providers. Of these firms, a majority conduct due diligence on such third-parties' cyber security practices. However, the extent of due diligence practiced by such firms varies greatly – some firms require third parties to provide them with copies of their policies and procedures on cyber security practices; some firms include terms about cyber security in their written agreements; some firms rely on standard of care clauses regarding the confidentiality/privacy of data and information; and others simply rely on the size and reputation of the third party without conducting an in-depth review.
- **Data Protection.** A sizeable number of firms do not use encryption to protect data and sensitive information from unauthorized access. The remainder of firms use encryption on various devices, including office computers, email communication and portable electronic devices.
- **Insurance**. A majority of firms (59%) do not have specific cyber security insurance, even though 51% of same have experienced a cyber security incident in 2016. Furthermore, the types of incidents and amounts that the cyber security insurance policies cover vary widely among firms which have purchased such insurance.
- **Social Media Policies and Procedures.** The majority of firms have policies and procedures that address social media practices, including guidelines on the appropriate and inappropriate use of social media (59%) and on permitted content, prohibited content, and restricted content created via social media (52%). 36% of firms provide employee training specifically related to social media use.
- **Social Media Monitoring.** A minority of firms (14%) engage in real-time monitoring of social media activity. Firms that do monitor social media activity do so through spot checks (46%), sample reviews of social media use by employees (29%), the use of lexicon-based or other search methodologies (11%) and specific software (17%).

Guidance

In light of the results noted above, the Staff Notice provides specific guidance for firms as to how to adequately respond to and prevent cyber and social media risks. This guidance included in the Staff Notice includes the following:

- **Policies and procedures.** A firm's policies and procedures should be designed to safeguard the confidentiality, integrity and availability of the firm's data, including client personal information. These policies and procedures should address, among other things, (i) use of electronic communications, (ii) use of firm-issued electronic devices, (iii) ensuring software is updated in a timely manner, and (iv) reporting cyber security incidents to the board of directors. With respect to the use of social media, a firm's policies and procedures should include (i) guidelines on the appropriate use of social media, (ii) procedures for ensuring that social media content is current, (iii) record keeping requirements, and (iv) review and approvals of social media content. Further guidance can be found in CSA Staff Notice 31-325.

- **Training**. Since employees are often the first line of defence against an attack, adequate training in the firm's cyber security practices is crucial to a firm's readiness to deal with cyber threats or incidents. The CSA note that, given the dynamic and ever-changing nature of the cyber world, including the evolution of cyber threats, training for cyber threats and cyber security practices should take place with sufficient frequency to remain current (i.e., more than annual training may be necessary).
- **Risk assessments.** A firm should conduct cyber security risk assessments at least annually which (i) inventory the firm's critical assets and confidential data, (ii) determine which areas of the firm's operations are vulnerable to cyber threats, (iii) identify potential consequences of the types of cyber threats identified, and (iv) assess the adequacy of the firm's preventative controls and incident response plan.
- **Incident response plans**. A firm should have a written incident response plan to respond to and to escalate a cyber security incident, which should include, among others, (i) who is responsible for communicating the cyber security incident, (ii) who should be involved in incident response, (iii) procedures to stop the incident from continuing to inflict damage, and (iv) identification of parties that should be notified.
- **Due diligence.** Written agreements with third parties should include provisions related to cyber threats, including a requirement by third party to notify firms of cyber security incidents resulting in unauthorized access to the firm's networks or data and the response plan of the third parties to counter these incidents. Furthermore, firms that rely on a cloud service should have procedures in place in the event that data on the cloud is not accessible.
- **Data protection**. Encryption is key. It protects the confidentiality of information as only authorized users can view the data. In addition to using encryption for all computers and other electronic devices, the CSA emphasize that a firm should require passwords (with different types of characters that must be frequently changed) to gain access to these devices.
- **Insurance**. A firm should review its existing insurance policies to identify which types of cyber security incidents, if any, are covered. For areas not covered by existing policies, a firm should consider whether additional insurance should be obtained.
- **Social media**. A firm should review, supervise, retain and have the ability to retrieve social media content, and have appropriate approval and monitoring procedures for social media communications. Even if a firm does not permit the use of social media for business purposes, policies and procedures should be in place to monitor for unauthorized use. See CSA Staff Notice 31-325 for further guidance on the use of social media.
- **Additional guidance.** Regardless of its size or functions outsourced, a firm should have cyber security policies and procedures, and in particular, a cyber security incident response plan that is tested on a regular basis.

Next Steps

The CSA have indicated that they will continue to review the cyber security and social media practices of firms through compliance reviews. In doing so, they will assess whether the guidance provided in the Staff Notice is being applied.