OSLER

# CSA issues guidance on cybersecurity and social media practices for registered firms

**OCTOBER 26, 2017 5 MIN READ**

## Related Expertise

- Cybersecurity and Security Incident Response
- Investment Management
- Privacy and Data Management

Authors: Adam Kardash, Blair Wiley

Registered dealers, advisers and investment fund managers are facing an increasing array of sophisticated threats to the security of their data holdings, including personal information in their custody and control.

The Canadian Securities Administrators (CSA) have accordingly identified cybersecurity as a priority area in the CSA's 2016-19 Business Plan, and have continued their focus in this area with the release of specific guidance regarding cybersecurity and social media practices.

CSA Staff Notice 33-321 Cyber Security and Social Media [PDF] (the Staff Notice), published on October 19, 2017, states that cybersecurity policies and procedures of registered firms should include preventative practices, training of all staff and a cybersecurity incident response plan. The CSA notes that the financial industry is a known target of cyber criminals, and therefore cybersecurity safeguards are internal controls which all registrants must adopt as part of their compliance systems in order to manage risk in accordance with prudent business practices.

## Background

CSA Staff Notice 11-332 Cyber Security [PDF], published in September 2016, advised registrants that their cybersecurity policies and procedures would be discussed during compliance reviews and described surveys and focus groups initiated by CSA members in order to gather data regarding the cybersecurity practices and training programs of registered firms.

The Staff Notice summarizes results of a survey completed in the fall of 2016 which solicited information from over 1,000 registrants, of which 63% responded. Approximately 51% of the responding firms had experienced a cybersecurity incident, including phishing, malware and attempted identity thefts in which a fraudster sought to transfer funds or securities of a client by impersonating the client via email.

## Cybersecurity

The Staff Notice sets out the CSA's expectations for each registrant to maintain: (i) cybersecurity policies and procedures which govern the use of electronic communications and devices, network security and the verification of client instructions sent electronically; (ii) frequent training of all employees, including with respect to risk recognition, types of cyber threats and incident escalation; (iii) an annual risk assessment process; (iv) an incident response plan; (v) oversight of the cybersecurity practices of service providers that have

access to firm networks or data; (vi) data protection safeguards, including the use of encryption and passwords on all computers and electronic devices; and (vii) insurance that adequately covers cybersecurity risks.

Based on the survey results set out in the Staff Notice, a majority of registrants will need to enhance their cybersecurity practices in the areas of data protection and insurance in order to meet CSA Staff expectations. Of the firms surveyed, only 48% reported the use of encryption to protect data on portable electronic devices, office computers, data files and/or email communications and attachments and almost 60% of firms reported that they do not have specific cybersecurity insurance. Although the CSA guidance does not explicitly require registrants to use encryption and obtain specific cybersecurity insurance, firms that do not adopt practices in accordance with the CSA's baseline expectations should be prepared to explain their alternative approaches toward managing the cybersecurity risks addressed by such practices.

In addition, 34% of survey respondents did not have an incident response plan in place, and 25% of firms that had response plans had not yet tested their plans. CSA Staff expect an incident response plan to allocate responsibility to specific personnel, describe different types of attacks, include procedures to mitigate damage, eradicate the threat and recover data, and be tested at least annually. Firm policies and procedures should provide for the reporting of cyber incidents and threats to the board of directors or governing body.

## Social media

Staff Notice 33-321 identifies social media as a vehicle for carrying out cyberattacks, such as the launch of targeted phishing emails or the provision of links to websites that install malware. Consequently, although social media policies generally focus on marketing as described in CSA Staff Notice 31-325 Marketing Practices of Portfolio Managers [PDF], registrants are also expected to consider cybersecurity issues when developing and monitoring these policies.

Survey results found that 77% of responding registrants had social media policies and procedures and 94% of responding registrants engaged in some type of social media monitoring. The Staff Notice identified room for improvement regarding employee training, recordkeeping and "take-down" guidelines for outdated posts on social media platforms.

CSA Staff emphasize the importance of approval and monitoring procedures given the ease with which information may be posted on social media platforms, the difficulty of removing posted information and the need to respond in a timely manner when issues arise. The CSA expects all firms to review, supervise, retain and have the ability to retrieve social media content, including monitoring for unauthorized social media communications by employees at firms which do not permit the use of social media for business purposes.

## Cybersecurity guidance for issuers

In February 2017, Staff from the British Columbia Securities Commission, the Ontario Securities Commission and the Autorité des marchés financiers du Québec published Multilateral Staff Notice 51-347: Disclosure of cyber security risks and incidents [PDF], which provided guidance to Canadian issuers regarding their disclosure practices. See our Osler Update for a summary of that multilateral staff notice.

## Conclusion

CSA Staff state that their cybersecurity guidance applies to all registered firms regardless of their size, how recently they were registered or the extent to which they rely on service providers or affiliates for their cybersecurity safeguards. The Staff Notice includes links to resources developed by Investment Industry Regulatory Organization of Canada [PDF] (IIROC), the Mutual Fund Dealers Association (MFDA) and the Office of the Superintendent of Financial Institutions (OSFI) to assist firms to self-assess their existing cybersecurity practices.

## How we can help

Osler regularly advises organizations in all sectors (including the financial services sector) on information security and data governance, including with respect to the development of incident readiness and response protocols. We have acted on the largest security incidents to date. With our internationally recognized and leading expertise in both security regulatory compliance and privacy and data protection, our team can provide you with practical, inter-disciplinary assistance in this rapidly evolving and complex area.

For more information please contact Lori Stein, Blair Wiley or Adam Kardash.