1.1.2 CSA Staff Notice 33-321 Cyber Security and Social Media

CSA/ACVM Canadian Securities Administrators Autorités canadiennes en valeurs mobilières

CSA Staff Notice 33-321
Cyber Security and Social Media

October 19, 2017

Introduction

Staff of the Canadian Securities Administrators (**CSA staff** or **we**) conducted a survey of cyber security and social media practices from October 11, 2016 to November 4, 2016. Cyber threats and social media pose growing risks for registered firms. These risks are complex, constantly evolving and widespread. The survey was designed to gather information from firms registered as investment fund managers, portfolio managers and exempt market dealers, to note trends and to form the basis for providing guidance about cyber security and social media practices.

Under section 11.1 of National Instrument 31-103 *Registration Requirements, Exemptions and Ongoing Registrant Obligations* (**NI 31-103**), a registered firm is required to establish, maintain and apply policies and procedures that establish a system of controls and supervision to ensure compliance with securities legislation and manage the risks associated with its business in accordance with prudent business practices. These compliance systems should address the risks of cyber threats and the use of social media, both of which pose risks for all registered firms. We previously highlighted in CSA Staff Notice 11-332 *Cyber Security* the importance of addressing cyber security risks and communicated our expectation that registered firms remain vigilant in developing, implementing and updating appropriate measures to safeguard themselves and their clients from cyber threats. We also stated that CSA staff will discuss cyber security policies and procedures with registered firms as part of compliance reviews.

As previously outlined in CSA Staff Notice 31-325 *Marketing Practices of Portfolio Managers* (**CSA Staff Notice 31-325**), there are compliance and supervisory challenges facing firms using social media as a means of communicating with clients and the general public, including an increased risk that registered firms may not be retaining adequate records of their business activities and client communications when using social media platforms. Section 11.5 of NI 31-103 requires a registered firm to maintain accurate records of its business activities, financial affairs and client transactions.

Additionally, firms should consider cyber security risks associated with social media use. For example, information posted on social media sites, for business or personal purposes, may be used by attackers to gain entry into a firm's systems and obtain confidential information.

This notice, in addition to setting out the results of the survey, is intended to provide more specific guidance to firms by suggesting policies and procedures in the areas of cyber security and social media practices. All registered firms should adopt cyber security and social media practices that include preventative practices, training to all staff and a response plan for when a cyber security incident occurs.

Survey

The survey was sent to over 1,000 registered firms and 63% of firms responded.

The survey questions were structured to gather information about:

- the firm's policies and procedures on cyber security and social media practices, including details about who is responsible for these areas and what training is provided to a firm's employees;
- the risk assessments conducted by the firm to identify cyber threats, vulnerabilities and potential consequences;
- cyber security incidents the firm experienced;
- the firm's cyber security incident response plan;

- the due diligence conducted by the firm to assess the cyber security practices of third-party vendors, consultants, or other service providers;
- the firm's data or system encryption policies and procedures and its backup process; and
- how the firm monitors its social media activities, including guidelines on appropriate content and record keeping.

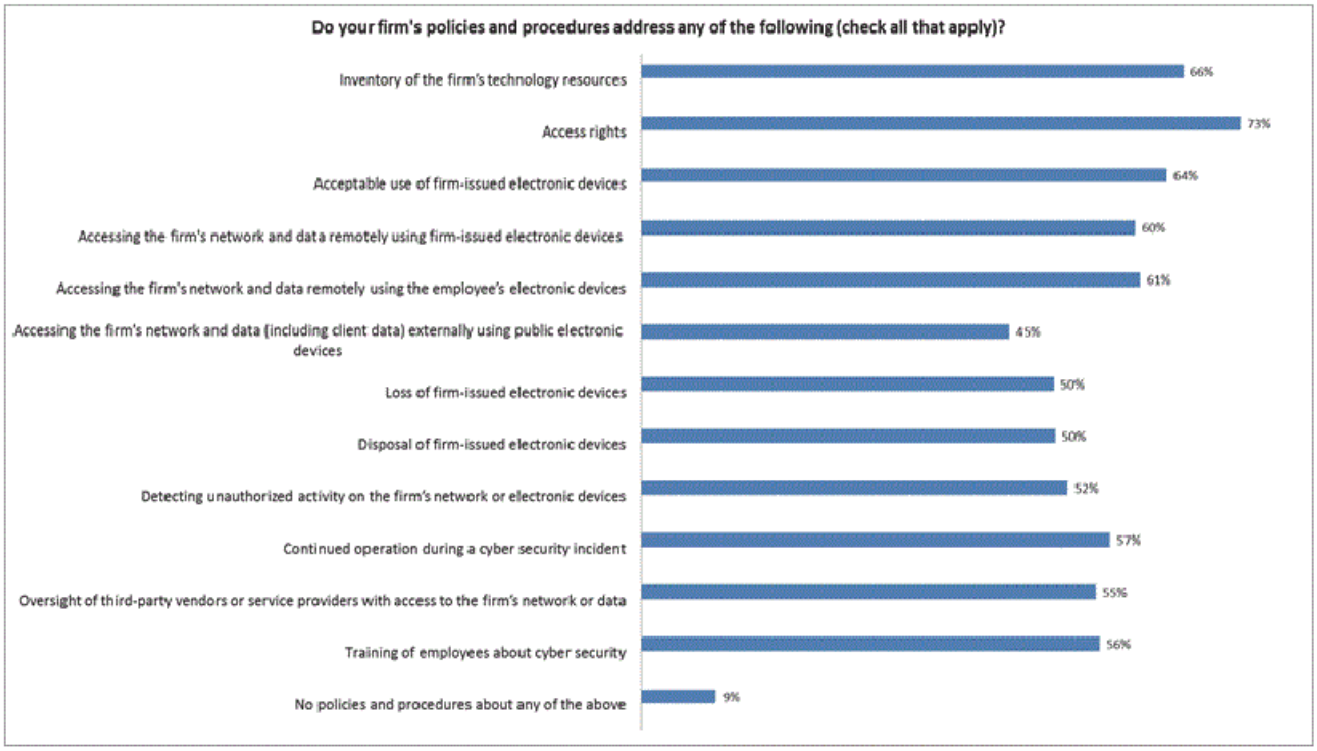
Summary of Survey Results and Guidance

A. Cyber security

Approximately 51% of firms experienced a cyber security incident in the year surveyed. Firms that experienced a cyber security incident indicated that the most common incident was phishing (43% of firms). Malware incidents were reported by 18% of firms and 15% of firms had experienced an attempt to impersonate a client to transfer funds or securities of that client using fraudulent email. Mitigating cyber threats is important to the firm's ability to manage its risks.

1. Policies and procedures

Most firms have policies and procedures to address cyber security. However, 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.



Guidance:

For firms to effectively implement their cyber security practices and provide training to employees on these practices, they should have policies and procedures that address the following areas:

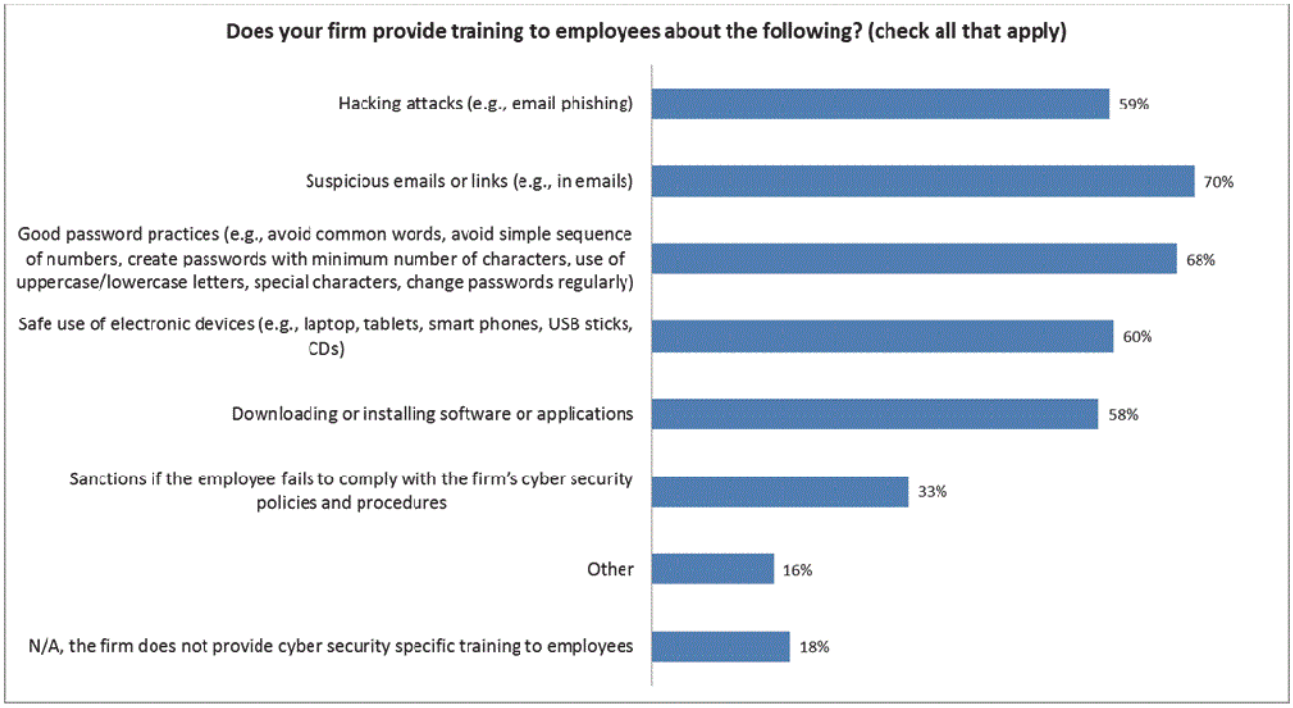
- use of electronic communications, including types of information that may be collected or sent through email, use of secured or unsecured communication systems and the verification of client instructions sent electronically;
- use of firm-issued electronic devices, including the use of such devices to externally access the firm's network and data;

- the loss or disposal of an electronic device, including electronic storage devices;
- use of public electronic devices or public internet connections to remotely access the firm's network and data, including to access client communications or client information;
- detecting internal or external unauthorized activity on the firm's network or electronic devices (e.g., hacking attempts, phishing or suspicious emails, malware);
- ensuring software, including anti-virus programs, is updated in a timely manner;
- overseeing third-party vendors or service providers with access to the firm's network or data (e.g., vetting, confidentiality); and
- reporting any cyber security incidents to the board of directors (or equivalent).

A firm's policies and procedures should be designed to safeguard the confidentiality, integrity and availability of the firm's data, including the personal information of clients. To stay up-to-date with changing cyber threats, firms should review and update these policies and procedures frequently.

2. Training

Where firms provide training to employees, the focus is on suspicious emails or links, good password practices and the safe use of hardware or software.



Guidance:

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. Employees should be educated on the risks associated with the data they may collect, use or disclose and the safe use of all electronic devices. Training can be conducted by the firm itself, or the firm can make training programs available through a third party.

Given the dynamic and ever-changing nature of the cyber world, including the possibility of new 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) and include topics such as:

- recognizing risks;
- types of cyber threats that employees may encounter (e.g., phishing) and how to respond to those threats;
- handling confidential firm and/or client information;
- use of passwords;
- security of all electronic devices; and
- when and how to escalate cyber security incidents.

3. Risk assessments

Most firms perform risk assessments at least annually to identify cyber threats. However, 14% of firms indicated that they do not conduct this type of assessment.

In response to the above question, most firms that answered "other" indicated that they conduct this risk assessment on an ongoing basis (e.g., ongoing monitoring via software, third-party service provider, or their parent company), or in some cases they conduct risk assessments at a different frequency (e.g., bi-annually or as needed, such as a result of any changes to hardware or software).

Guidance:

At least annually, registered firms should conduct a cyber security risk assessment. The risk assessment should include:

- an inventory of the firm's critical assets and confidential data, including what should reside on or be connected to the firm's network and what is most important to protect;
- what areas of the firm's operations are vulnerable to cyber threats, including internal vulnerabilities (e.g., employees) and external vulnerabilities (e.g., hackers, third-party service providers);
- how cyber threats and vulnerabilities are identified;
- potential consequences of the types of cyber threats identified; and
- adequacy of the firm's preventative controls and incident response plan, including evaluating whether changes are required to such a plan.

4. Incident response plan

A significant number of firms (66%) have a cyber security incident response plan that is tested at least annually. As noted in the chart below, the frequency of testing of the incident response plans vary and many firms have not tested their plans.

Firms that indicated "other" test their cyber security incident response plan at a different frequency (e.g., bi-annually or as needed, such as a result of any changes), or indicated that their cyber security incident response plan was scheduled to be tested in the coming year.

Guidance:

Firms should have a written incident response plan to respond to and to escalate a cyber security incident. The incident response plan should include:

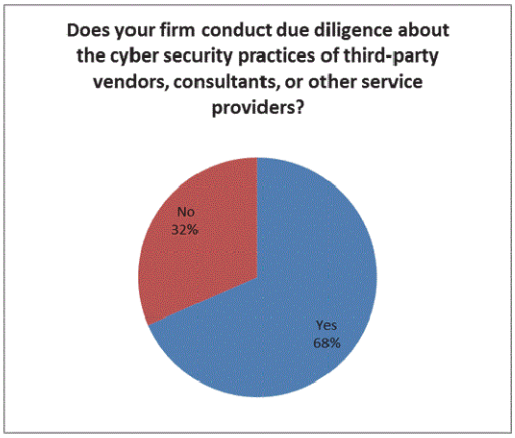
- who is responsible for communicating about the cyber security incident and who should be involved in the response to the incident;
- a description of the different types of cyber attacks (e.g., malware infections, insider threats, cyber-enabled fraudulent wire transfers) that might be used against the firm;
- procedures to stop the incident from continuing to inflict damage and the eradication or neutralization of the threat;
- procedures focused on recovery of data;
- investigation of the incident to determine the extent of the damage and to identify the cause of the incident so the firm's systems can be modified to prevent another similar incident from occurring; and
- identification of parties that should be notified and what information should be reported.

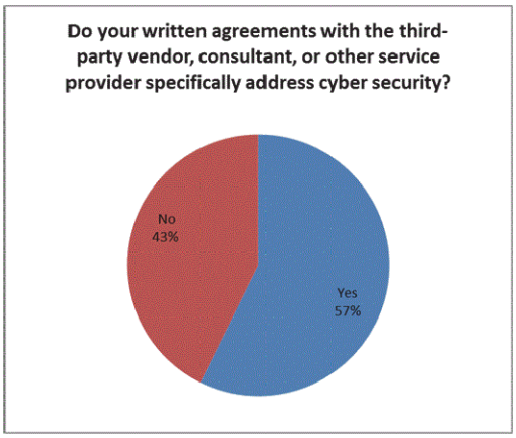
5. Due diligence

A significant number of firms surveyed (92%) have engaged third-party vendors, consultants, or other service providers (e.g., an IT provider, custodian, record keeper, transfer agent, valuation agent). Of these firms, a majority conduct due diligence on the cyber security practices of these third parties.

The extent of the due diligence conducted and how it is documented vary 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.

A majority of firms indicated that their written agreements with third-party vendors, consultants, or other service providers specifically address cyber security.





Some firms indicated that they will conduct due diligence going forward and include terms in their written agreements that are specific to cyber security as they update their existing agreements or when they enter into new ones.

Guidance:

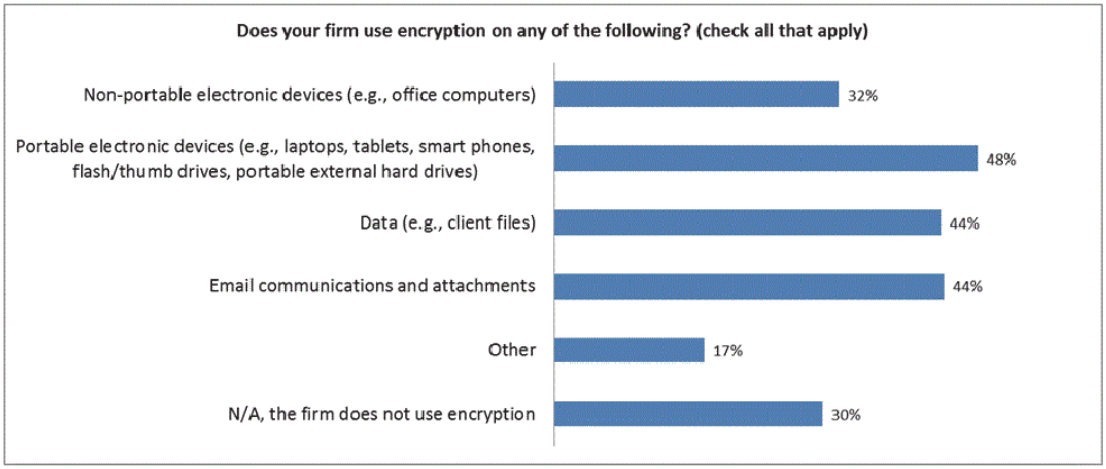
Firms should evaluate, on a periodic basis, the adequacy of their cyber security practices, including safeguards against cyber security incidents and the handling of such incidents by any third parties that have access to the firms' systems and data. In addition, firms should limit the access of third-party vendors to their systems and data.

Written agreements with these outside parties should include provisions related to cyber threats, including a requirement by third parties to notify firms of cyber security incidents resulting in unauthorized access to the firms' networks or data and the response plans of the third parties to counter these incidents.

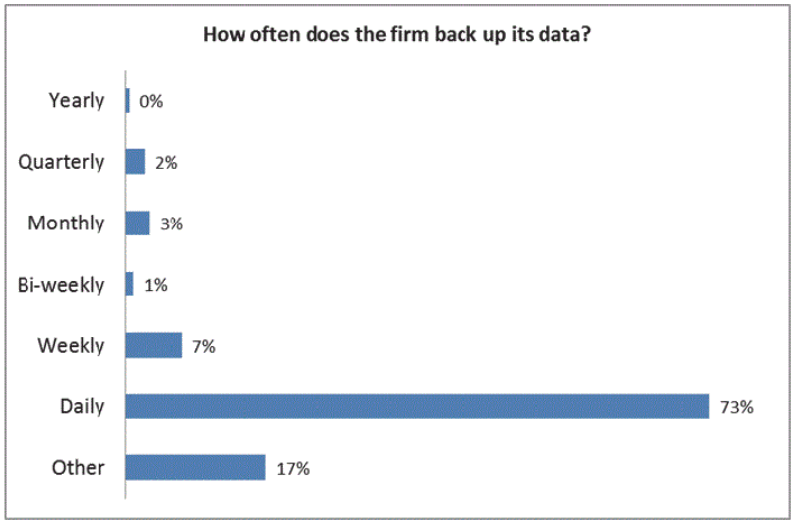
Where firms use cloud services, they should understand the security practices that the cloud service provider has to safeguard from cyber threats and determine whether the practices are adequate. Firms that rely on a cloud service should have procedures in place in the event that data on the cloud is not accessible.

6. Data protection

Client data can be stored or accessed through various technologies such as email, cloud storage and websites. Encryption is one of the tools firms can use to protect their data and sensitive information from unauthorized access. As indicated in response to the question below, a sizeable number of firms do not use any encryption or rely on other methods of data protection, such as password protected documents.



Except for four firms, all firms that responded to the survey indicated that they back up data on a periodic basis. Of the firms that back up their data, 73% perform backups on a daily basis and 89% have tested their backup recovery process.



Some firms that indicated "other" back up their data a number of times daily (e.g., in some cases hourly), or they answered "other" because the frequency depends on the type of data (e.g., data or systems deemed critical are backed up every 15 minutes, while other non-critical data is backed up daily, weekly, etc.).

A significant number of firms provide their clients and third parties (e.g., dealers, service providers) with access to the firms' data or systems. However, this access is not always through secure channels.

Guidance:

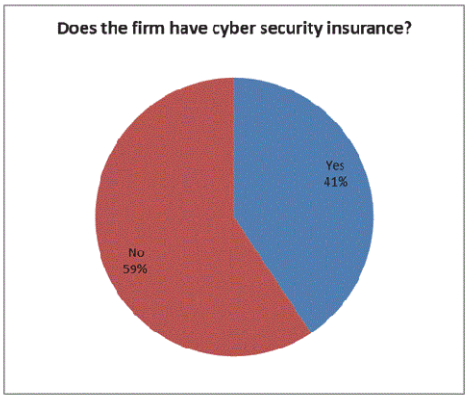
Encryption protects the confidentiality of information as only authorized users can view the data. In addition to using encryption for all computers and other electronic devices, firms should require passwords to gain access to these devices. Stronger passwords require different types of characters (e.g., numbers, uppercase letters and symbols) and are required to be frequently changed.

Where firms provide portals for clients or other third parties for communication purposes or for accessing the firm's data or systems, firms should ensure the access is secure and data is protected.

We expect firms to back up their data and regularly test their back-up process. Also, when backing up data, firms should ensure that the data is backed up off-site to a secure server in case there is physical damage to the firms' premises.

7. Insurance

A majority of firms (59%) do not have specific cyber security insurance. The types of incidents and amounts that these policies cover vary widely among firms that have purchased cyber security insurance.



Guidance:

Firms should review their existing insurance policies (e.g., financial institution bonds) to identify which types of cyber security incidents, if any, are covered. For areas not covered by existing policies, firms should consider whether additional insurance should be obtained.

Additional comments

Some small firms or newly-registered firms indicated that they believe their cyber security risk to be low because of their size. As a result, they did not believe they need to develop cyber security policies and procedures or provide training to employees. However, the financial industry is a known target of cyber criminals. In addition, other firms indicated that they rely on the safeguards provided by their parent company or service providers (e.g., custodian, transfer agent, cloud service provider). 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.

Cyber Security Resources

CSA Staff Notice 11-332 *Cyber Security* included a list of reference documents prepared by various regulatory authorities and standard-setting bodies that may be useful to firms, including the following:

- Investment Industry Regulatory Organization of Canada (IIROC) Cybersecurity Best Practices Guide
  http://www.iiroc.ca/industry/Documents/CybersecurityBestPracticesGuide_en.pdf

- IIROC Cyber Incident Management Planning Guide
  http://www.iiroc.ca/industry/Documents/CyberIncidentManagementPlanningGuide_en.pdf

- Mutual Fund Dealers Association (MFDA) Bulletin #0690-C
  http://www.mfda.ca/regulation/bulletins16/Bulletin0690-C.pdf

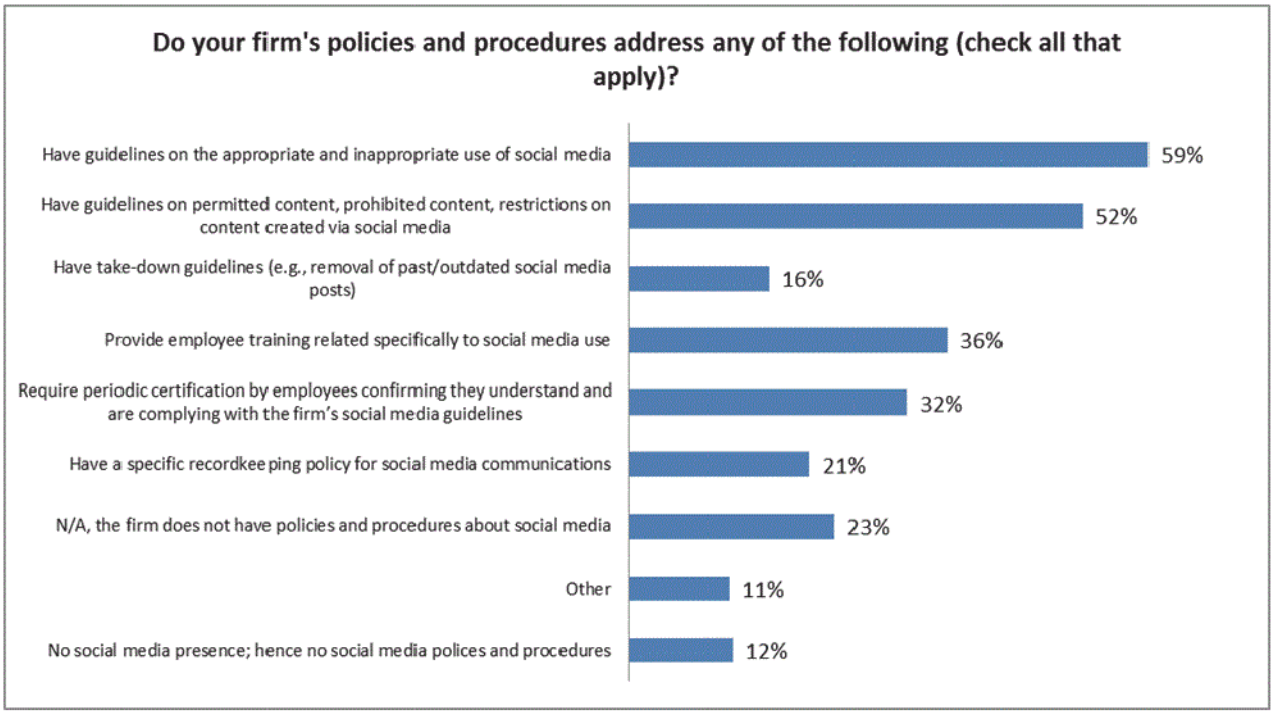
- The Office of the Superintendent of Financial Institutions (OSFI) Cyber Security Self-Assessment Guidance
  http://www.osfi-bsif.gc.ca/eng/fi-if/in-ai/pages/cbrsk.aspx

B. Social Media

Social media may be used as a vehicle to carry out cyber attacks. For example, social media sites may be used by attackers to launch targeted phishing emails or links on these sites may lead to websites that install malware. Although the survey results and guidance outlined below focus on social media used for marketing, they should also be considered in the context of cyber security.

1. Policies and procedures

Most firms have policies and procedures on social media practices. While 59% of firms surveyed have guidelines on the appropriate and inappropriate use of social media, only 36% have policies and procedures about the training of employees specifically about social media use and 21% have specific recordkeeping policies for social media communications.



Guidance:

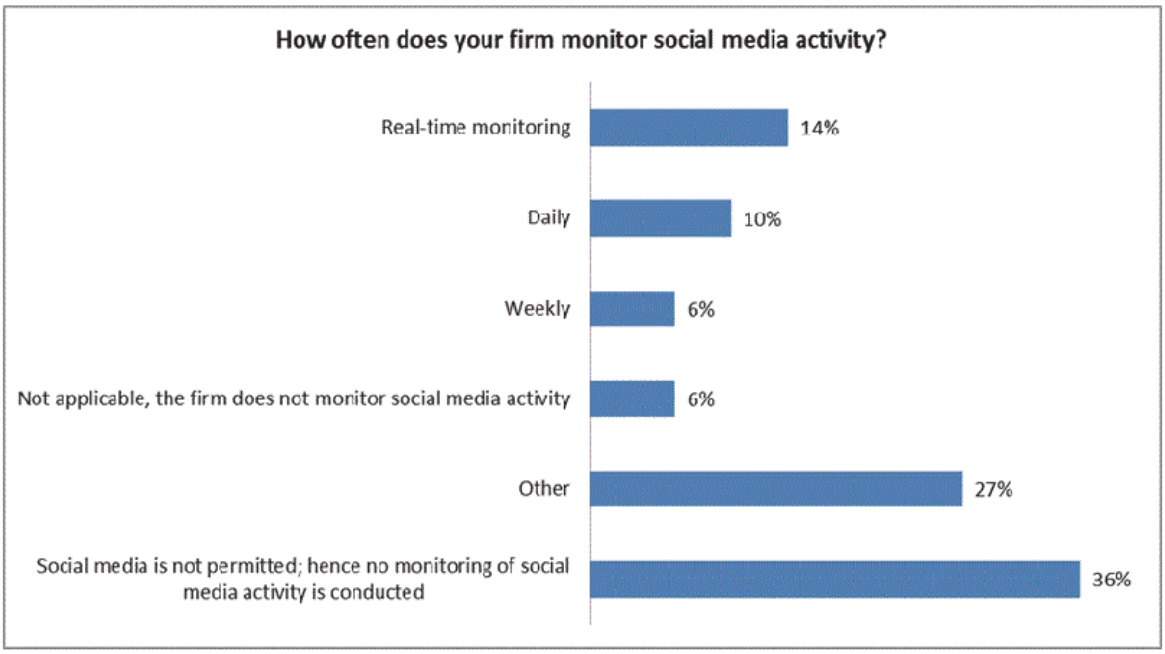
Firms should review, supervise, retain and have the ability to retrieve social media content. Policies and procedures on social media practices should include:

- guidelines on the appropriate use of social media, including the use of social media for business purposes;
- guidelines on what content is permitted when using social media;
- procedures for ensuring that social media content is current;
- record keeping requirements for social media content; and
- reviews and approvals of social media content, including evidence of such reviews and approvals.

Firms should also review CSA Staff Notice 31-325 for further guidance on the above.

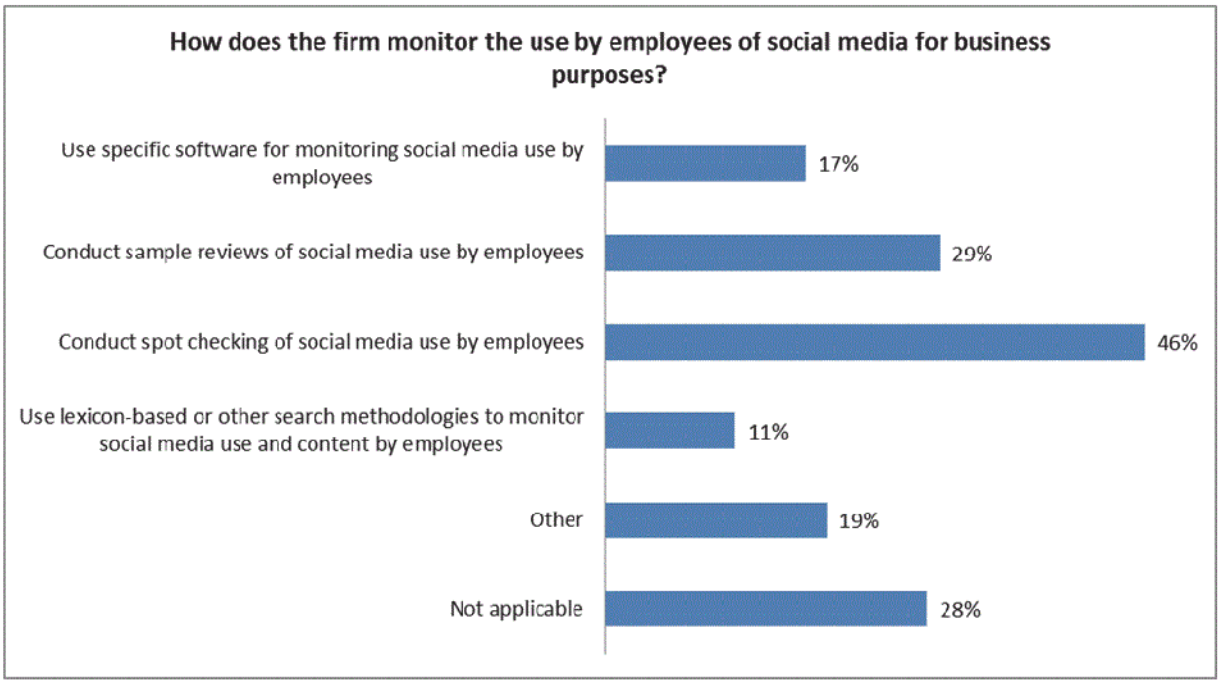
2. Monitoring of social media activity, including supervision of employees' use of social media for business and personal purposes

Only a small percentage of firms (14%) engage in real-time monitoring of social media activity. A small segment of firms do not monitor social media activity at all (6%).



Some firms that indicated "other" in response to the above question monitor social media on an annual, quarterly or monthly basis, or periodically as needed.

In order to monitor the use by employees of social media for business purposes, 46% of firms conduct spot checking or a sample review.



Guidance:

Given the ease with which information may be posted on social media platforms, the difficulty of removing information once posted and the need to respond in a timely manner to issues that may arise, firms should have appropriate approval and monitoring procedures for social media communications. Even if firms do not permit the use of social media for business purposes, policies and procedures should be in place to monitor for unauthorized use.

For further guidance on the use of social media, we refer firms to CSA Staff Notice 31-325.

Next Steps

CSA staff will continue to review the cyber security and social media practices of firms through compliance reviews. CSA staff will apply the information and guidance in this notice when assessing how firms comply with their obligations to manage the risks associated with their business as set out in NI 31-103.

Questions

Please refer your questions to any of the following:

Curtis Brezinski
Compliance Auditor, Capital Markets, Securities Division
Financial and Consumer Affairs Authority of Saskatchewan
306-787-5876
curtis.brezinski@gov.sk.ca

Angela Duong
Compliance Auditor
Manitoba Securities Commission
204-945-8973
angela.duong@gov.mb.ca

Reid Hoglund
Regulatory Analyst
Alberta Securities Commission
403-297-2991
reid.hoglund@asc.ca

To-Linh Huynh
Senior Analyst
Financial and Consumer Services Commission (New Brunswick)
506-643-7856
to-linh.huynh@fcnb.ca

Éric Jacob
Directeur principal de l'inspection
Autorité des marchés financiers
514-395-0337, extension 4741
eric.jacob@lautorite.qc.ca

Janice Leung
Manager, Adviser/IFM Compliance
British Columbia Securities Commission
604-899-6752
jleung@bcsc.bc.ca

Susan Pawelek
Accountant
Compliance and Registrant Regulation Branch
Ontario Securities Commission
416-593-3680
spawelek@osc.gov.on.ca

Chris Pottie
Manager, Compliance and SRO Oversight
Policy and Market Regulation Branch
Nova Scotia Securities Commission
902-424-5393
chris.pottie@novascotia.ca

Craig Whalen
Manager of Licensing, Registration and Compliance
Office of the Superintendent of Securities
Newfoundland and Labrador
709-729-5661
cwhalen@gov.nl.ca