CSA/ACVM Canadian Securities Administrators Autorités canadiennes en valeurs mobilières

CSA Staff Notice 33-322

Review of Registered Firms' Cybersecurity Practices and Additional Guidance

July 15, 2026

INTRODUCTION

Under section 11.1 of National Instrument 31-103 *Registration Requirements, Exemptions and Ongoing Registrant Obligations* (**NI 31-103**), a firm registered under Canadian securities legislation as a dealer, adviser, or investment fund manager (a **registered firm** or **firm**) is required to establish, maintain and apply policies and procedures that establish a system of controls and supervision sufficient to manage the risks associated with its business in accordance with prudent business practices. These compliance systems should address the risk of cyber threats, which is a risk for all registered firms.

Staff of the Canadian Securities Administrators (**CSA**) (**Staff** or **we**) are publishing this staff notice (the **Notice**) to summarize the findings of our recent focused compliance examinations of registered firms' cybersecurity practices, to provide additional guidance on regulatory expectations, and to serve as an important reminder to firms that cybersecurity threats are a critical business risk.

BACKGROUND

Following the COVID-19 pandemic, Canada finds itself in a more technology-centric world than ever before, and that is reflected in the operations of our registered firms. Many registered firms have employees working remotely on personal and corporate devices, are using cloud-based applications to hold firm information, communicate with their clients via email and video calls, and some even perform key functions, such as the collection of know your client information, via online platforms. With these technological advances and a greater online presence also comes an increased risk of a firm being affected by cybersecurity threats, which are becoming increasingly prevalent and sophisticated.

Registered firms' cybersecurity practices are examined by Staff during routine compliance examinations. In 2017, Staff published CSA Staff Notice 33-321 *Cyber Security and Social Media* (**CSA Staff Notice 33-321** or the **2017 guidance**) that discussed the results of a cybersecurity survey issued to registered firms. However, given the increasing importance of strong cybersecurity practices, starting in July 2025, Staff began focused compliance examinations to review the cybersecurity policies and procedures that registered firms have in place to protect firm and confidential client information. The aim of these focused examinations was to identify some

notable areas where firms could strengthen their cybersecurity practices, observe current best practices, and use these insights to inform updated guidance.

EXAMINATIONS

Staff conducted compliance examinations of a sample of 73 firms as part of this focused cybersecurity sweep. The sample included firms registered in the categories of investment fund manager, portfolio manager, restricted portfolio manager, exempt market dealer, and combinations thereof.

Staff's examinations focused on whether registered firms' cybersecurity practices satisfy section 11.1 of NI 31-103. At a high-level, Staff expected firms to have adequate:

(1) cybersecurity policies and procedures;
(2) cybersecurity training;
(3) cybersecurity risk assessment processes (with respect to both identification of risk areas and the associated effective controls);
(4) due diligence of third-party service providers; and
(5) cybersecurity incident response plans.

Deficiencies were raised if Staff noted a concern in one of these areas or in the documentation supporting one of these areas, in accordance with section 11.5 of NI 31-103.

In addition to CSA Staff Notice 33-321, our examinations were also guided by earlier CSA cybersecurity notices:

- from 2016 (CSA Staff Notice 11-332 *Cyber Security*); and
- from 2013 (CSA Staff Notice 11-326 *Cyber Security*).

This Notice is intended to complement, update, and expand on this past guidance. For ease of reference, we have reproduced select excerpts from the 2017 guidance within this Notice. However, we strongly recommend that firms also review CSA Staff Notice 33-321 in its entirety as it provided the foundation for this Notice.

A number of firms that we examined, particularly larger firms, had robust cybersecurity policies and procedures. Accordingly, this Notice may be particularly helpful for smaller or medium-sized firms seeking to enhance their cybersecurity frameworks. Staff recognize that firms of different sizes and complexities are not expected to address cybersecurity in the same way, provided that relevant cybersecurity risks are appropriately addressed. For smaller firms with less complex operations, these practices may be implemented in a simpler form, while larger, more complex firms are generally expected to have more detailed frameworks.

The goal of this guidance is to serve as a reminder that cybersecurity incidents are a business risk to registered firms, and a risk to confidential client data held by these firms. Staff expect firms to have robust cybersecurity practices relevant to the firm's business. Firms should also stay up to

date on, and appropriately address, shifting cybersecurity needs that may arise due to the continually evolving cyber landscape. Registered firms may be subject to cybersecurity obligations under other laws and regulations that are not described in this Notice. It is the registered firm's responsibility to comply with any cybersecurity obligations that apply to the firm.

SUMMARY OF RESULTS

This section sets out our examination findings, as well as provides some effective practices, general observations, and key takeaways that may be helpful for registered firms.

1. <u>Cybersecurity policies and procedures</u>

Most firms had written cybersecurity policies and procedures, though the adequacy of these policies and procedures varied across firms.

Staff found:

- 8% of firms did not have any written cybersecurity policies and procedures.
- 55% of firms had written cybersecurity policies and procedures that could be further enhanced.

Staff generally found that firms' cybersecurity policies and procedures could be enhanced by sufficiently addressing important areas relevant to the firm's business. In making these observations, Staff considered the 2017 guidance (see excerpt below). For example, Staff found that some firms did not have adequate policies and procedures relating to the use of electronic communications and the loss or disposal of electronic devices.

Excerpt from 2017 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 [critical] cyber security incidents to the board of directors (or equivalent).

In addition to the above, it was noted that cybersecurity policies and procedures could be enhanced where the following areas were not addressed, if applicable to the firm:

- ***Cybersecurity risk assessments*** – Staff expect cybersecurity risk assessments to be a standard practice at registered firms. We expect firms' policies and procedures to specify that cybersecurity risk assessments will be conducted and to outline, at a level of detail appropriate to the firm's size and complexity, when they will be conducted, who is responsible, and the steps involved.

- ***Website and application usage*** – Staff expect firms to have policies and procedures that address the use of external websites and applications by employees, as applicable.

- ***Use of privately owned electronic devices*** – With increased work-from-home and remote access to firm systems and data, firms should have appropriate policies and procedures to address employee use of personal devices (phones, laptops, etc.) to access firm systems and data. These policies and procedures should specifically address that personal devices do not have the same security controls as firm-issued devices and, accordingly, appropriate limits should be set on how personal devices may connect to and access firm systems and data. This ties in with a need for policies and procedures governing the use of public internet connections when remotely accessing the firm's systems and data from personal devices.

- ***Data security and encryption*** – Staff expect to see policies and procedures addressing how confidential data is secured and protected, including with respect to the use of cloud storage. If a firm offers an online client portal, it should have policies and procedures to safeguard the confidential information on that portal.

- ***Employee cybersecurity training and awareness*** – Staff have an expectation that cybersecurity training be conducted for a registered firm's employees. Firms' policies and procedures should address cybersecurity training for employees, including details of the process at the firm (e.g., frequency, scope, responsibility).

- ***Accountability for cybersecurity*** – Registered firms should clearly set out in their policies and procedures who (what teams, individuals, etc.) is responsible for overseeing the different components of the firm's cybersecurity policies and procedures.

Other findings Staff noted with respect to firms' cybersecurity policies and procedures were:

- **Cybersecurity policies and procedures were not reviewed and updated with sufficient frequency.** Due to the continually evolving cyber threat landscape, Staff generally expect

cybersecurity policies and procedures to be reviewed and updated frequently and at least annually. There should be documentation of this review.

- **Firms' cybersecurity policies and procedures did not match their actual firm practices.** Staff noted instances where a firm's actual practices (which may have been adequate) were inconsistent with what was set out in the firm's written policies and procedures (e.g., policies and procedures note that the firm's cybersecurity incident response plan would be tested twice a year but in practice it was only tested annually). Where such inconsistencies were observed, Staff raised a deficiency.

Key takeaways for firms

- *Firms should have comprehensive written cybersecurity policies and procedures that address, at a minimum, the key areas set out above, as well as any additional areas applicable to the firm's business based on the firm's size and nature of the operations.*
- *Firms should review and update their cybersecurity policies and procedures at least annually and maintain documentation of this review.*
- *Firms should confirm that their cybersecurity policies and procedures align with the firm's operations.*

2. Cybersecurity training

Most firms provided cybersecurity training to employees, and Staff found many of these training programs to be comprehensive.

Staff found:

- 21% of firms did not provide any cybersecurity training to their employees.
- 21% of firms that provided training could have provided more comprehensive training.
- 16% of firms that provided training had no documentation or limited documentation to support the cybersecurity training provided to their employees.

Staff found that some firms' cybersecurity training could be strengthened to address key cybersecurity risk areas. In making these observations, Staff considered the areas highlighted in the 2017 guidance (see excerpt below). Staff also found cybersecurity training provided was not sufficient where the firm did not provide adequate cybersecurity training on an ongoing basis (e.g., where the training at the time of onboarding was comprehensive, but the firm did not provide any further or periodic training to employees).

Excerpt from 2017 guidance –

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.

Other observations noted in relation to cybersecurity training are discussed below.

Oversight and delivery of cybersecurity training

The responsibility for developing and delivering cybersecurity training varied across firms, ranging from fully in-house programs to those supported or entirely implemented by third-party service providers. Staff observed that most firms relying on third-party service providers to deliver training maintained internal oversight of the training. This oversight was often exercised by the firm's Chief Compliance Officer, compliance staff, or a senior technology lead, and included review and approval of training materials. Staff consider this to be prudent as the responsibility for providing adequate cybersecurity training that is comprehensive and relevant to the firm's specific operations remains with the registered firm, even if it is outsourced. Staff are of the view that it is a best practice for training to be tailored to the specific risks employees are most likely to encounter at the firm and in their roles.

Firms delivered cybersecurity training in a variety of ways, such as through live presentations or webinars, using pre-recorded virtual sessions, as well as written materials. Some firms have their employees complete a test at the completion of the training to ensure that their employees understand the materials.

Frequency and timing of cybersecurity training

Staff generally expect cybersecurity training to be provided at least annually. However, as noted in the 2017 guidance above, cybersecurity training should be sufficiently frequent to remain current, and more than annual training sessions may be necessary depending on the firm and its operations. For example, firms with greater operational complexity (e.g., large workforce, multiple business locations) or a heightened cyber risk for other reasons (e.g., deals with high volume of sensitive client data, uses multiple third-party service providers with access to firm systems and data, permits remote or hybrid work arrangements), should consider providing training more frequently than once a year.

In addition, Staff noted a best practice of firms requiring cybersecurity training upon onboarding of new employees, particularly when such training was required to be completed within a certain timeframe of the employee joining the firm (e.g., within one month of joining). As noted above, Staff do not find it sufficient for cybersecurity training to occur only during employee onboarding with no ongoing training.

Social engineering simulation tests

In addition to more traditional training modules, many firms used phishing and other social engineering simulation tests, in some cases multiple times annually, to mimic real cyber threat scenarios and assess employee responses. These practical tests, which can be conducted by third-party service providers, can be an effective way to test employee understanding of cybersecurity training and awareness of how to respond to cyber threats.

A best practice that Staff observed was for firms to automatically assign additional training to any individual who failed a social engineering simulation test (e.g., clicked on a malicious link), with escalating interventions for repeated failures (e.g., notifying the individual's manager, and then involving human resources or a cybersecurity lead at the firm). Firms noted that the objective of such testing was not only for employees to avoid incorrect actions, but to ensure employees can recognize and report suspicious activity to the firm's Information Technology (IT) or appropriate senior staff, so that others can be protected from the same threat in a real-life scenario.

Documentation of cybersecurity training

Firms should maintain records to demonstrate that cybersecurity training took place, including who attended, the date it occurred, and the content covered. As noted above, some firms were found to have no documentation or limited documentation to support the cybersecurity training provided to employees. Some firms with inadequate documentation indicated that training was conducted informally (e.g., during team meetings).

If firms are employing phishing or other social engineering simulation tests as part of their cybersecurity training, Staff consider it a best practice for firms to be able to demonstrate that these tests took place, including records of employee responses and any follow-up actions.

Key takeaways for firms

- *Cybersecurity training should address, at a minimum, the key areas set out above, as well as any additional areas applicable to the firm's business based on the firm's size and nature of the operations.*
- *Firms should provide cybersecurity training on at least an annual basis and with sufficient frequency to remain current (more than annual training may be necessary).*
- *Firms should consider conducting periodic testing to assess employees' ability to recognize and report suspicious activity, and consider using targeted training to address any outcomes that do not meet expectations.*

- *If cybersecurity training is outsourced to a third-party service provider, designate individual(s) at the firm to oversee the cybersecurity training program so that it is appropriate for the firm's specific operations.*
- *Firms should maintain records to demonstrate that cybersecurity training took place, including who attended, the date it occurred, and the content covered.*

3. Cybersecurity risk assessments & controls

While some firms conducted comprehensive cybersecurity risk assessments annually or more frequently (e.g., quarterly or semi-annually), Staff found that a number of firms' cybersecurity risk assessments could have been strengthened, including where the assessments did not adequately address key areas or were not supported by sufficient documentation.

Staff found:

- 45% of firms conducted cybersecurity risk assessments during the examination period that could have been more robust.
- 12% of firms had no documentation of a cybersecurity risk assessment during the examination period. Staff also noted that many firms could have improved their cybersecurity risk assessment documentation.

Staff generally found that a firm's cybersecurity risk assessment, or its related documentation, could have been strengthened if it did not adequately address key elements relevant to the firm's business. In making these observations, Staff considered the areas outlined in the 2017 guidance (see excerpt below). For example, Staff found that a number of firms did not adequately address the following:

(1) areas of the firm's operations that are vulnerable to cybersecurity threats (these are a firm's cybersecurity risk areas and may include, at a high level, a firm's devices, data, electronic mail, websites, and applications);
(2) how cybersecurity threats and vulnerabilities are identified;
(3) potential consequences of the types of cybersecurity threats identified; and
(4) adequacy of the firm's preventative controls to address the firm's risk areas.

Excerpt from 2017 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.

Firms should document their risk assessments, including associated controls. Staff expect the documentation to demonstrate that the firm has sufficiently considered the areas noted above.

Staff also raised cybersecurity risk assessment deficiencies specifically with respect to (1) employee access rights not being addressed as a risk area and (2) firms relying solely on third-party service providers to conduct the cybersecurity risk assessments, as discussed below.

(1) Employee access rights

Staff raised a deficiency when employee access rights (i.e., an employee's access to a firm's systems, data, etc.) was not identified as a risk area, and if the risk was not addressed with adequate controls in the firm's cybersecurity risk assessment.

Examples of effective controls we observed to address the risk of employee access rights included:

- Role-based access controls, where an employee's access to systems and data was tied to the role assigned to the employee (e.g., by the firm's human resources department). When an employee changed roles or left the organization, access rights were updated or terminated within a set timeframe. Further, when assigning access rights to a particular role, it can be effective to consider the "principle of least privilege", meaning employees should only have the level of access needed to complete their tasks, and not more.
- Oversight measures for access rights, such as requiring manager review or approval where appropriate and conducting periodic reviews of all employee access rights, particularly in larger firms with more employees, to confirm access remains appropriate.

With respect to access rights, Staff noted deficiencies where controls existed in design but were not supported by effective monitoring and detection mechanisms. Firms should consider whether their cybersecurity controls operate effectively in practice to identify and respond to unauthorized access or activity in a timely manner.

(2) Reliance on third-party service providers

We noted that some firms relied on third-party service providers to conduct cybersecurity risk assessments for the firm and provide the firm with a summary of the results (e.g., highlighting areas of high risk at the firm where there were no or inadequate controls in

place). Staff do not have concerns with the use of third parties to conduct risk assessments; however, firms are expected to:

a) review the risk assessment prepared by the third-party service provider;
b) evaluate the adequacy of the risk assessment and address any missing elements; and
c) set out how any cybersecurity concerns identified by the third-party service provider have been or will be addressed.

Where firms did not have documentation showing that they completed this review, Staff raised a deficiency.

Staff noted that some firms that engaged third-party service providers to assist with their cybersecurity risk assessments were able to conduct risk assessments more frequently than annually, which may help strengthen a firm's cybersecurity regime.

In addition to a firm's cybersecurity risk assessment, Staff noted that effective complementary practices included firms engaging third-party service providers to perform cybersecurity audits and penetration testing. Though not a requirement, engaging a third-party service provider to review or simulate cyber attacks to test a firm's cybersecurity regime can be an effective way to identify vulnerabilities and any potential gaps in controls. We observed an instance where a firm alternated third-party service providers engaged to assess cyber risks, to gain diverse perspectives on potential vulnerabilities.

General controls to consider to address risk areas

Staff expect firms to implement controls to address the risk areas identified in their cybersecurity risk assessments. Firms should identify the controls that are in place or will be in place to address the firm's risk areas, and evaluate the adequacy of these controls, in the documentation of their cybersecurity risk assessments.

Staff have highlighted below some basic controls to prevent, detect, and mitigate cybersecurity risks that firms should consider implementing if they have not done so already. *We note that this is not an exhaustive list and is meant to help firms consider how they might improve their cybersecurity regime*.

- Use complex passwords (with minimum requirements for length and varied characters, set out when updates are required, etc.).
- Use multi-factor authentication to add an additional verification step, beyond a password, before logging into the firm's systems.
- Use virtual private networks (VPN) to secure remote connections to the firm's systems.
- Use data encryption (in transit and at rest) to protect sensitive information from unauthorized access or disclosure.

- Maintain scheduled system backups with defined frequencies, retention, and testing procedures to ensure recoverability.
- Use security tools (i.e., firewalls and endpoint security) that block unauthorized access to the firm's systems.
- Implement email filtering to block spam, phishing attempts, and malicious attachments before they reach users.
- Use regular patching and software updates to provide timely fixes that address security vulnerabilities.
- Remove unnecessary software or applications from firm devices to reduce exposure to cybersecurity risks.
- Maintain logs of suspicious cyber activity to proactively monitor for potential cybersecurity incidents.
- Securely wipe sensitive data prior to equipment disposal or reuse.

Key takeaways for firms

- *Firms should conduct cybersecurity risk assessments at least annually and the assessment should cover, at a minimum, the key areas set out above, as well as any additional areas applicable to the firm's business based on the firm's size and nature of the operations.*
- *The cybersecurity risk assessment should be documented, and this documentation should include the controls in place to address the firm's risk areas as well as an evaluation of the adequacy of the controls.*
- *If a third-party service provider is conducting, or assisting with, a cybersecurity risk assessment for a firm, the firm should maintain documentation showing that it (a) reviewed the third-party assessment, (b) evaluated its adequacy and added any missing elements, and (c) addressed or has a plan to address any concerns identified.*

4. Third-party service providers

All firms reviewed in our examinations used third-party service providers that had access to firm systems or data, including firms that use cloud-based service providers to store their firm and client data.

Staff are aware of cybersecurity incidents that occurred at third-party service providers used by registered firms, where those service providers had access to the firm's confidential data. Although these incidents were not a breach of the registered firms' own systems, these types of incidents could compromise a firm's confidential information, including personal client details, similar to if the breach had occurred at the registered firm itself.

Accordingly, it is important that firms recognize the use of third-party service providers as a cybersecurity risk area in their cybersecurity risk assessments. Firms should establish and document adequate controls to address this risk.

As touched on in the 2017 guidance (see excerpt below), firms should conduct and document sufficient initial and ongoing cybersecurity due diligence on their prospective and current third-party service providers, respectively. In our examinations, Staff found:

- 41% of firms could strengthen their cybersecurity oversight of third-party service providers.
- 62% of firms had no documentation or limited documentation to support their cybersecurity oversight of third-party service providers.

Excerpt from 2017 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.

Meaningful due diligence on third-party service providers

Staff expect firms to conduct and document meaningful due diligence on the cybersecurity practices of their third-party service providers to satisfy themselves that the cybersecurity practices of the service provider are adequate. The due diligence should be conducted before onboarding a service provider and on a sufficiently frequent basis for as long as the service provider is engaged.

Staff are of the view that this includes conducting and documenting an appropriate level of due diligence on the cybersecurity practices of technology companies, including widely known and established companies, engaged by the firm, that may provide services such as business email, document management, infrastructure, and other technological services to the registered firm. However, the level of due diligence necessary may differ depending on the nature of the service provider. For example, firms should conduct more detailed cybersecurity due diligence for the firm's critical business service providers (e.g., a fund accountant, client reporting service provider, transfer agent, etc.).

Information gathering in due diligence process

Information that firms may consider gathering from third-party service providers as part of their cybersecurity due diligence on those providers includes information on the provider's:

- cybersecurity policies and procedures, including whether the provider follows any recognized cybersecurity standards;
- data handling practices (including where and in what manner firm data may be stored, and the use of encryption in transit and at rest);
- physical and legal locations for operations, the requirements applicable to the service provider based on its jurisdiction, and any potential risks arising from this;
- access controls;

- vulnerability and patch management processes;
- physical security practices;
- incident detection and response protocols for a cybersecurity incident, including how and when the firm would be notified if affected;
- management of past cybersecurity incidents;
- management of its third-party service providers;
- frequency with which it completes a cybersecurity risk assessment (e.g., if it is done on a regular basis); and
- expectations for how security responsibilities are divided between the service provider and the firm, so it is clear who is responsible for protecting systems and data in a shared cloud environment.

Due diligence practices observed

Some practices observed that firms may consider implementing as part of their cybersecurity due diligence of third-party service providers include:

- using a cybersecurity questionnaire for engaging third-party service providers, and updating these questionnaires on a sufficiently frequent basis (e.g., annually) once the service provider has been engaged;
- obtaining attestations from third-party service providers as to how the registered firm's systems and data are protected;
- maintaining a log of all their third-party service providers and supporting due diligence documentation; and
- receiving and reviewing cybersecurity reporting from third-party service providers on a periodic basis.

In our examinations, for the firms that received cybersecurity reporting from third-party service providers:

- The reporting was most often received and reviewed annually.
- The most common form of reporting received and reviewed was the third-party service providers' System and Organization Controls (**SOC**) reports. In particular, SOC 2 reports assess a company's security controls and are typically prepared annually. When conducting initial and ongoing due diligence on third-party service providers, firms should consider requesting a recent SOC 2 or similar report for review, where available.
- The reporting was also provided in other forms, such as the following:
    - an updated cybersecurity due diligence questionnaire on the service provider;
    - an updated cybersecurity risk assessment conducted on the service provider; and
    - the service provider's current cybersecurity incident response plan.

Key takeaways for firms

- *Firms should conduct meaningful due diligence on the cybersecurity practices of third-party service providers to be satisfied that the cybersecurity practices of the service provider are adequate. This due diligence should be conducted before onboarding the third-party service provider and be done on a sufficiently frequent basis while the service provider is engaged.*
- *Firms should maintain adequate documentation to show the cybersecurity due diligence performed on third-party service providers.*

5. Cybersecurity incident response plan

We noted that some firms had a documented definition of a "cybersecurity incident", while others did not. In Staff's view, setting out a definition for what constitutes a "cybersecurity incident" is an important first step in developing an effective cybersecurity incident response plan (an **incident response plan**), as it informs when the plan should be activated.

Where firms had defined a "cybersecurity incident", those definitions generally included the following:

- an event that could compromise the confidentiality, integrity, or availability of the firm's systems, data, or services;
- an event that involves the potential or actual unauthorized disclosure of sensitive information, such as personal identification information, financial information, or firm records about individuals or third-party entities;
- unauthorized access or attempted access to a firm's systems;
- an event that occurs by accident or deliberately that impacts the firm's systems and data (including potential misuse, theft, loss, disclosure, destruction, or modification);
- an event that may result in harm or inconvenience to clients and creates a threat of loss or disruption to business operations, reputation, or assets; and
- an event that has been determined to have an impact on the firm, prompting the need for response and recovery.

Staff found:

- 15% of firms did not have a written incident response plan at all.
- 53% of firms with a written incident response plan could have had a stronger incident response plan.
- 63% of firms with a written incident response plan should have tested their plan on a more regular basis.

Previous guidance on written incident response plans, data backups, and cybersecurity insurance is noted below:

Excerpt from 2017 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.

…

We expect firms to back up their data and regularly test their back-up process.

…

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.

…

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.

Creating an incident response plan

Staff generally found that a firm's written incident response plan could be further strengthened if the plan did not address certain key elements for an effective incident response. In making these observations, Staff considered the 2017 guidance (see excerpt above). For example, Staff found that a number of firms' written incident response plans did not include a description of the different types of cyber attacks that might be used against the firm.

Cybersecurity incidents at third-party service providers with access to a firm's systems or data can have the same or a similar impact on confidential firm information as incidents that occur at the registered firm itself. Accordingly, we also found a firm's written incident response plan could be

further strengthened to include procedures for responding to a cybersecurity incident at a third-party service provider that has access to the firm's systems or data. Staff expect firms to document in their incident response plans how they will respond if notified of a cybersecurity incident at one of their third-party service providers.

Data backup and recovery

Staff observed deficiencies where firms did not regularly test data backups or did not retain records supporting their testing. As part of prudent cybersecurity practices, firms should: consider whether they maintain appropriate backup arrangements given the size and complexity of the firm; conduct appropriate periodic backup recovery testing; and retain records supporting their backup recovery testing and their ability to restore data in a timely manner.

Cybersecurity insurance

62% of firms indicated to Staff that they have a cybersecurity insurance policy. In addition to this, some firms that did not have separate cybersecurity insurance policies indicated that the firm is covered for cybersecurity incidents under other insurance policies.

Though cybersecurity insurance is not required, Staff are of the view that obtaining this insurance coverage can be beneficial, as it can help reduce financial harm to a firm when faced with a cybersecurity incident and an insurance provider's steps and operational assistance may also help guide firms through dealing with a cybersecurity incident (e.g., assist the firm with engaging cybersecurity breach counsel or other qualified specialists, if necessary).

Testing incident response plans

Given the persistent challenges posed by cybersecurity threats and the rapidly evolving nature of the cyber threat landscape, as noted in the 2017 guidance, Staff expect firms to test their incident response plans on a regular basis. There should be documentation to support the testing.

Testing a firm's incident response plan is important as it can help ensure that the firm, and particularly, the firm's teams and individuals involved in the response, are prepared to respond efficiently and effectively to a cybersecurity incident. Testing can help key individuals become more prepared to respond in a real cyber incident scenario and can also help firms identify potential gaps in their incident response plan that should be addressed.

There are a variety of ways that a firm can test its incident response plan, including through:

- **Tabletop exercises:** Discussion-based walkthroughs of hypothetical cybersecurity incident scenarios. The key individuals involved in the incident response talk through the different steps of the response, as set out in the firm's incident response plan. The adequacy of the incident response plan can then be assessed.

- **Simulated attack testing:** These are technical, hands-on cybersecurity exercises where attackers and defenders work together to see how well the firm and its systems can detect and respond to real-world cyber threats. These exercises can help assess how technical cybersecurity controls are operating and the adequacy of the incident response plan.

These tests can be conducted in-house or through engaging third-party service providers.

Key takeaways for firms

- *Firms should have a written incident response plan that is comprehensive and addresses, at a minimum, the key areas set out above, as well as any additional areas applicable to the firm's business based on the firm's size and nature of the operations.*
- *Firms should back up their data and regularly conduct backup recovery testing. Firms should retain records supporting their backup recovery testing and their ability to restore data in a timely manner.*
- *Firms should test their incident response plan on a regular basis and maintain documentation to support the testing.*

QUESTIONS

Please refer your questions to any of the following Staff:

Zulqer Khan
Lead, Market Regulation IT Projects
Alberta Securities Commission
403-297-5036
zulqer.khan@asc.ca

Aneri Mehta
Regulatory Analyst, Registrant Oversight
Alberta Securities Commission
403-355-2269
aneri.mehta@asc.ca

Jason Donovan
Inspecteur coordonnateur
Direction du service de l'inspection -- valeurs mobilières
Autorité des marchés financiers
514-395-0337 (4756)
jason.donovan@lautorite.qc.ca

Jason Chan
Senior Compliance Analyst
Adviser/IFM Compliance, Capital Markets Regulation
British Columbia Securities Commission
604-899-6735
jchan@bcsc.bc.ca

Crystal He
Lead Compliance Analyst, Capital Markets Regulation
British Columbia Securities Commission
604-899-6795
che@bcsc.bc.ca

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

Michelle Doucette
Compliance Officer, Securities Division
Financial and Consumer Services Commission
of New Brunswick
506-721-5223
michelle.doucette@fcnb.ca

Aishah Abdullahi
Compliance Auditor
Manitoba Securities Commission
204-945-8973
aishah.abdullahi@gov.mb.ca

Angela Duong
Deputy Director, Compliance and Oversight
Manitoba Securities Commission
204-945-5195
angela.duong@gov.mb.ca

Cynthia Tambago-Alday
Deputy Director, Registration & Compliance
Nova Scotia Securities Commission
902-424-5393
cynthia.tambago-alday@novascotia.ca

Samantha Cardinale
Legal Counsel, Registration, Inspections and Examinations
Ontario Securities Commission
416-597-7230
scardinale@osc.ca

Alizeh Khorasanee
Head of Dealer Compliance, Registration, Inspections and Examinations
Ontario Securities Commission
416-716-3307
akhorasanee@osc.ca

Susan Pawelek
Senior Accountant, Registration, Inspections and Examinations
Ontario Securities Commission
416-593-3680
spawelek@osc.ca