3.1

Avis et communiqués

3.1 AVIS ET COMMUNIQUÉS

Avis de publication

Avis 33-322 du personnel des Autorités canadiennes en valeurs mobilières : *Examen des pratiques de cybersécurité des sociétés inscrites et indications supplémentaires*

(Avis publié ci-dessous)

CSA/ACVM Canadian Securities Administrators Autorités canadiennes en valeurs mobilières

Avis 33-322 du personnel des ACVM

Examen des pratiques de cybersécurité des sociétés inscrites et indications supplémentaires

Le 15 juillet 2026

INTRODUCTION

L'article 11.1 du *Règlement 31-103 sur les obligations et dispenses d'inscription et les obligations continues des personnes inscrites* (le **Règlement 31-103**) prévoit que la société inscrite en vertu de la législation en valeurs mobilières à titre de courtier, de conseiller ou de gestionnaire de fonds d'investissement (une **société inscrite** ou une **société**) doit établir, maintenir et appliquer des politiques et des procédures instaurant un système de contrôles et de supervision suffisant pour gérer les risques liés à son activité conformément aux pratiques commerciales prudentes. Ces systèmes de conformité devraient encadrer le risque lié aux cybermenaces, auquel sont exposées toutes les sociétés inscrites.

Le personnel des Autorités canadiennes en valeurs mobilières (les **ACVM**) (le **personnel** ou **nous**) publie le présent avis pour résumer ses constatations issues des récentes inspections ciblées de la conformité des pratiques de cybersécurité des sociétés inscrites, fournir des indications supplémentaires concernant les attentes réglementaires et rappeler aux sociétés que les menaces à la cybersécurité constituent un risque commercial critique.

CONTEXTE

Depuis la pandémie de COVID-19, la technologie est plus présente que jamais au Canada, et les sociétés inscrites n'échappent pas à cette réalité dans leurs activités. Bon nombre d'entre elles comptent des employés en télétravail utilisant un appareil personnel ou fourni par l'employeur, ont recours à des applications infonuagiques pour stocker leur information et communiquent avec leurs clients par courriel ou appel vidéo. Certaines se servent même de plateformes en ligne pour effectuer des tâches clés, comme la collecte de renseignements relatifs à la connaissance du client. Ces avancées technologiques, conjuguées à une présence en ligne accrue, ne sont pas sans accroître l'exposition aux menaces à la cybersécurité, lesquelles sont de plus en plus répandues et complexes.

Le personnel examine les pratiques de cybersécurité des sociétés inscrites à l'occasion d'inspections courantes de la conformité. En 2017, il a publié l'Avis 33-321 du personnel des ACVM, *Cybersécurité et médias sociaux* (l'**Avis 33-321** ou les **indications de 2017**), qui traitait des résultats d'un sondage sur la cybersécurité mené auprès de sociétés inscrites. Cependant, vu l'importance croissante des pratiques de cybersécurité rigoureuses, le personnel a entrepris, en juillet 2025, la réalisation d'inspections ciblées de la conformité axées sur les politiques et

procédures de cybersécurité mises en place par ces sociétés pour protéger leur information ainsi que les renseignements confidentiels des clients. Ces inspections avaient pour but de cerner des aspects notables où les sociétés pourraient renforcer leurs pratiques, d'observer les pratiques exemplaires actuelles et d'utiliser ces données pour mettre à jour les indications.

INSPECTIONS

Dans le cadre des inspections ciblées en matière de cybersécurité, le personnel a utilisé un échantillon de 73 sociétés. Ce dernier comprenait des sociétés inscrites dans une ou plusieurs des catégories suivantes : gestionnaire de fonds d'investissement, gestionnaire de portefeuille, gestionnaire de portefeuille d'exercice restreint et courtier sur le marché dispensé.

Le personnel a cherché à déterminer, à l'aide des inspections, si les pratiques de cybersécurité des sociétés inscrites répondaient aux dispositions de l'article 11.1 du Règlement 31-103. Globalement, il s'attendait à ce que les sociétés soient dotées :

1) de politiques et de procédures de cybersécurité adéquates;
2) de formations appropriées en la matière;
3) de processus pertinents d'évaluation du risque lié à la cybersécurité (en ce qui concerne la définition des éléments de risque et des contrôles efficaces connexes);
4) de contrôles diligents satisfaisants à l'égard des tiers fournisseurs de services;
5) de plans d'intervention efficaces en cas d'incident de cybersécurité.

Le personnel a signalé des déficiences dans les cas où, au regard de l'article 11.5 du Règlement 31-103, il avait des craintes à l'égard de l'un de ces éléments ou de leur documentation.

En plus de l'Avis 33-321, d'autres avis antérieurs des ACVM traitant de cybersécurité ont guidé les inspections :

- l'Avis 11-332 du personnel des ACVM, *Cybersécurité* (2016);
- l'Avis 11-326 du personnel des ACVM, *Cybersécurité* (2013).

Le présent avis vient compléter, actualiser et élargir les indications publiées antérieurement. Pour faciliter la consultation, le personnel y a reproduit certains extraits de l'Avis 33-321. Cependant, comme elles ont servi de fondement au présent avis, il recommande fortement aux sociétés de les consulter dans leur intégralité.

Un certain nombre de sociétés inspectées, particulièrement les grandes sociétés, s'étaient dotées de politiques et procédures de cybersécurité solides. Par conséquent, le présent avis pourrait se révéler fort utile aux petites et moyennes sociétés cherchant à rehausser leur cadre de cybersécurité. Le personnel est conscient qu'il ne peut pas s'attendre à ce que des sociétés de taille et de complexité différentes abordent la cybersécurité de la même façon; il faut néanmoins que les risques pertinents en la matière soient traités convenablement. La mise en œuvre des pratiques de cybersécurité peut être élémentaire chez les petites sociétés au fonctionnement simple, tandis

qu'elle devrait généralement faire l'objet d'un cadre plus détaillé chez les grandes sociétés plus complexes.

Les indications fournies ci-après ont pour objet de rappeler que les incidents de cybersécurité font peser un risque commercial sur les sociétés inscrites et un risque sur les données confidentielles de leurs clients qu'elles détiennent. Le personnel s'attend à ce que ces sociétés appliquent des pratiques de cybersécurité rigoureuses et utiles dans le contexte de leurs activités. Elles devraient également se tenir au fait des besoins changeants en matière de cybersécurité qui peuvent découler de l'évolution constante du cyberespace, et y répondre de manière appropriée. Elles pourraient être assujetties à des obligations de cybersécurité en vertu d'autres lois et règlements qui ne sont pas décrits aux présentes. Il incombe à la société inscrite de se conformer aux obligations applicables en la matière.

RÉSUMÉ DES CONSTATATIONS

La présente rubrique expose les constatations issues de nos inspections ainsi que des pratiques efficaces, des observations d'ordre général et des éléments à retenir pouvant servir aux sociétés inscrites.

1. <u>Politiques et procédures de cybersécurité</u>

La plupart des sociétés avaient couché sur papier des politiques et des procédures de cybersécurité, quoique leur adéquation variait d'une société à l'autre.

Le personnel a fait les constatations suivantes :

- 8 % des sociétés n'avaient rédigé aucune politique ou procédure de cybersécurité;
- chez 55 % des sociétés, les politiques et procédures de cybersécurité écrites pourraient être rehaussées.

De manière générale, le personnel a constaté que les politiques et procédures de cybersécurité pourraient être rehaussées en abordant convenablement les éléments importants pour leurs activités. Il s'est appuyé sur les indications de 2017 pour formuler ses observations (voir l'extrait ci-dessous). Par exemple, il a noté que certaines sociétés ne disposaient pas de politiques ou de procédures adéquates relativement à l'utilisation des communications électroniques ainsi qu'à la perte ou à la destruction d'appareils électroniques.

Extrait des indications de 2017

Pour mettre en œuvre leurs pratiques en matière de cybersécurité et offrir de la formation à leurs employés, les sociétés devraient établir des politiques et des procédures encadrant les éléments suivants :

- l'utilisation des communications électroniques, notamment le type d'information pouvant être recueillie ou transmise par courriel, l'utilisation de systèmes de communications sécurisés ou non et la vérification des instructions du client transmises électroniquement;
- l'utilisation des appareils électroniques appartenant à la société, notamment pour accéder à distance à son réseau et à ses données;
- la perte ou la destruction d'un appareil électronique, notamment les dispositifs de stockage électroniques;
- l'utilisation d'appareils électroniques publics ou de connexions Internet publiques pour accéder à distance au réseau et aux données de la société, notamment pour accéder aux communications avec les clients ou à l'information sur ceux-ci;
- la détection des activités internes ou externes non autorisées sur le réseau ou les appareils électroniques de la société (par exemple, les tentatives de piratage, l'hameçonnage ou les courriels douteux, et les maliciels);
- l'assurance que les logiciels, notamment les programmes antivirus, sont mis à jour en temps opportun;
- la supervision des tiers fournisseurs, notamment de services, ayant accès au réseau ou aux données de la société (par exemple, au moyen d'un examen approfondi ou d'une entente de confidentialité);
- la déclaration de tout cyberincident [critique] au conseil d'administration (ou son équivalent).

En plus des éléments indiqués ci-dessus, les inspections ont permis de relever que les politiques et procédures pourraient être rehaussées dans les cas où les éléments suivants, s'ils s'appliquaient à la société, n'avaient pas été abordés :

- ***Évaluations du risque lié à la cybersécurité*** – Le personnel s'attend à ce que les évaluations du risque lié à la cybersécurité constituent une pratique courante des sociétés inscrites. Il compte que leurs politiques et procédures précisent que ces évaluations seront effectuées et qu'elles indiquent, de façon suffisamment détaillée selon la taille et la complexité de la société, le moment auquel elles auront lieu, les personnes responsables et les étapes prévues.

- ***Utilisation de sites Web et d'applications*** – Le personnel s'attend à ce que les sociétés disposent de politiques et de procédures traitant de l'utilisation que font les employés de sites Web et d'applications externes, le cas échéant.

- ***Utilisation d'appareils électroniques personnels*** – En raison de l'expansion du télétravail et de l'accès à distance aux systèmes et aux données d'entreprise, les sociétés devraient se doter de politiques et de procédures adéquates relativement à l'utilisation des appareils personnels (téléphones, ordinateurs portables, etc.) à cette fin. Ces politiques et procédures devraient préciser que les appareils personnels ne sont pas soumis aux mêmes contrôles de sécurité que ceux fournis par la société. Par conséquent, il y a lieu d'imposer aux appareils

personnels des restrictions appropriées quant au mode de connexion et d'accès aux systèmes et aux données de la société. De même, il convient de mettre en place des politiques et procédures régissant l'utilisation des connexions Internet publiques pour accéder à distance aux systèmes et aux données de la société par ces appareils.

- ***Sécurité et chiffrement des données*** – Le personnel s'attend à trouver des politiques et des procédures traitant de la sécurité et de la protection des données confidentielles, notamment en ce qui concerne l'utilisation du stockage infonuagique. Les sociétés proposant un portail client en ligne devraient s'être dotées de politiques et de procédures pour protéger l'information confidentielle qui y circule.

- ***Formation et sensibilisation des employés sur la cybersécurité*** – Le personnel estime que les sociétés inscrites devraient former leurs employés sur la cybersécurité. Leurs politiques et procédures devraient traiter de la formation sur la cybersécurité offerte aux employés, y compris le détail du processus (par exemple, la fréquence, la portée et la responsabilité).

- ***Reddition de comptes en matière de cybersécurité*** – Les sociétés inscrites devraient indiquer clairement, dans leurs politiques et procédures, qui sont les responsables (équipes, personnes physiques, etc.) de la surveillance des diverses composantes des politiques et des procédures de cybersécurité.

Le personnel a également fait les constatations suivantes à l'égard des politiques et des procédures de cybersécurité des sociétés :

- **La fréquence de la révision et de l'actualisation des politiques et des procédures de cybersécurité est insuffisante.** En raison de l'évolution constante des menaces à la cybersécurité, le personnel s'attend à ce que, de manière générale, les politiques et procédures de cybersécurité soient révisées et actualisées fréquemment, et au moins une fois par année. Le détail de la révision devrait être consigné en dossier.

- **Les politiques et procédures de cybersécurité de certaines sociétés ne concordent pas avec leurs pratiques réelles.** Dans certains cas, le personnel a remarqué que les pratiques réelles des sociétés (qui pouvaient être adéquates) ne cadraient pas avec leurs politiques et procédures écrites (par exemple, ces dernières indiquaient que le plan d'intervention en cas d'incident de cybersécurité serait mis à l'essai deux fois par année, alors que, dans les faits, il ne l'était qu'une seule fois). En pareil cas, le personnel a signalé une déficience.

Principaux éléments à retenir pour les sociétés

- *Les sociétés devraient s'être dotées de politiques et de procédures de cybersécurité écrites exhaustives qui traitent au moins des éléments clés mentionnés ci-dessus, ainsi que de tout autre élément applicable à leurs activités selon leur nature et la taille de la société.*
- *Les sociétés devraient réviser et actualiser leurs politiques et procédures de cybersécurité au moins une fois par année, et consigner en dossier le détail de ces révisions.*
- *Les sociétés devraient vérifier que leurs politiques et procédures de cybersécurité concordent avec leurs activités.*

2. Formation sur la cybersécurité

Le personnel a constaté que la plupart des sociétés offraient à leurs employés des programmes de formation sur la cybersécurité, dont un grand nombre étaient exhaustifs.

Le personnel a fait les constatations suivantes concernant la formation offerte aux employés sur la cybersécurité :

- 21 % des sociétés ne leur en fournissaient aucune;
- 21 % des sociétés qui leur en proposaient pourraient leur en fournir une plus étendue;
- 16 % des sociétés qui leur en proposaient ne disposaient que de peu, voire pas, de documentation étayant la formation offerte.

Le personnel a conclu que la formation sur la cybersécurité de certaines sociétés pourrait être renforcée afin d'aborder les principaux éléments de risque liés à la cybersécurité. Il s'est appuyé sur les indications de 2017 pour formuler ses observations (voir l'extrait ci-dessous). Il a également relevé que cette formation n'était pas suffisante dans les cas où la société ne fournissait pas de formation continue appropriée (par exemple, formation exhaustive offerte au moment de l'intégration de l'employé, mais aucune par la suite, périodique ou autre).

Extrait des indications de 2017

Compte tenu du dynamisme et de la constante évolution du cybermonde, notamment la possibilité de nouvelles cybermenaces, la formation devrait être offerte suffisamment souvent pour demeurer à jour (c'est-à-dire qu'il peut être nécessaire de l'offrir plus d'une fois par année) et aborder des sujets tels que :

- la reconnaissance des risques;
- les types de cybermenaces que les employés peuvent rencontrer (par exemple, l'hameçonnage) et les façons d'y réagir;
- le traitement des renseignements confidentiels de la société ou des clients;
- l'utilisation des mots de passe;
- la sécurité de tous les appareils électroniques;
- le moment et la façon de signaler les cyberincidents aux échelons supérieurs.

Figurent ci-après d'autres observations concernant la formation sur la cybersécurité.

Supervision et prestation de la formation sur la cybersécurité

La responsabilité à l'égard de l'élaboration et de la prestation de la formation sur la cybersécurité varie d'une société à l'autre, allant de programmes entièrement conçus en interne à ceux soutenus ou mis en œuvre intégralement par des tiers fournisseurs de services. Le personnel a constaté que la plupart des sociétés s'appuyant sur de tels fournisseurs pour assurer la formation conservaient à l'interne la supervision de celle-ci. Souvent, cette fonction revenait au chef de la conformité, au personnel du service de la conformité ou à un responsable principal de la technologie, et englobait l'examen et l'approbation du matériel didactique. Le personnel estime qu'il s'agit d'une approche prudente, car il incombe à la société inscrite d'offrir une formation sur la cybersécurité qui soit adéquate et exhaustive et concorde avec ses activités, même si elle est externalisée. Il considère également qu'il est une pratique exemplaire d'adapter la formation aux risques auxquels les employés sont le plus susceptibles d'être exposés dans leurs fonctions.

La formation sur la cybersécurité fournie par les sociétés prenait plusieurs formes, comme des présentations en direct ou des webinaires, des séances de formation virtuelles préenregistrées ainsi que des documents écrits. Certaines sociétés demandent à leurs employés de passer un test après la formation pour confirmer qu'ils l'ont bien comprise.

Fréquence et calendrier de la formation sur la cybersécurité

De façon générale, le personnel s'attend à ce que la formation sur la cybersécurité ait lieu au moins annuellement. Cependant, ainsi qu'il est indiqué dans l'extrait des indications de 2017 ci-dessus, la formation devrait être offerte suffisamment souvent pour demeurer à jour, et plus d'une séance par année pourrait être nécessaire, selon la société et ses activités. Par exemple, les sociétés au

fonctionnement plus complexe (entre autres, des effectifs nombreux ou de multiples établissements) ou confrontées à un cyberrisque accru pour d'autres raisons (par exemple, composant avec un volume élevé de données sensibles sur les clients, faisant appel à plusieurs tiers fournisseurs de services ayant accès à ses systèmes et données, ou autorisant le télétravail ou une formule de travail hybride) devraient envisager de fournir de la formation plus d'une fois par année.

En outre, le personnel a noté la pratique exemplaire consistant pour les sociétés à obliger les nouveaux employés à suivre une formation sur la cybersécurité lors de leur intégration, et particulièrement à la terminer dans un certain délai (par exemple, un mois) après leur arrivée. Comme il est indiqué ci-dessus, le personnel estime qu'il est insuffisant de former les employés sur la cybersécurité uniquement lors de leur accueil.

Simulations de piratage psychologique

Bon nombre de sociétés ont greffé aux modules de formation classiques des simulations d'hameçonnage et d'autres types de piratage psychologique, dans certains cas plusieurs fois par année, pour imiter des scénarios réels de cybermenaces et évaluer la réaction des employés. Ces simulations pratiques, parfois menées par des tiers fournisseurs de services, peuvent se révéler efficaces pour confirmer que les employés ont bien assimilé la formation sur la cybersécurité, et tester leur réponse à ces menaces.

Parmi les pratiques exemplaires observées chez les sociétés, le personnel souligne l'attribution automatique de formations additionnelles à toute personne ayant échoué une simulation de piratage psychologique (par exemple, si elle a cliqué sur un lien malveillant), ainsi que des démarches hiérarchiques en cas d'échecs répétés (par exemple, informer le gestionnaire de la personne en situation d'échec, puis demander l'intervention des ressources humaines ou d'un responsable en cybersécurité de la société). Les sociétés ont fait remarquer que l'objectif de ces simulations n'était pas seulement d'enseigner aux employés à éviter les faux pas, mais de faire en sorte qu'ils sachent reconnaître les activités suspectes et les signaler au service des technologies de l'information ou à un cadre supérieur concerné de la société afin de protéger leurs collègues contre une telle menace dans un cas réel.

Dossiers relatifs à la formation sur la cybersécurité

Les sociétés devraient tenir des dossiers démontrant que la formation sur la cybersécurité a eu lieu et renfermant le nom des participants, la date de la formation et les éléments abordés. Comme mentionné précédemment, certaines sociétés disposaient de dossiers limités, voire d'aucun, étayant la formation sur la cybersécurité offerte aux employés. Des sociétés ayant une documentation inadéquate ont indiqué que la formation était fournie de façon informelle (par exemple, lors de réunions d'équipe).

Si des sociétés procèdent à des simulations d'hameçonnage ou d'autres types de piratage psychologique dans le cadre de la formation sur la cybersécurité, le personnel estime qu'il s'agit d'une pratique exemplaire pour elles de pouvoir montrer que ces simulations ont eu lieu, ainsi que la réponse des employés et les mesures de suivi prises.

Principaux éléments à retenir pour les sociétés

- *La formation sur la cybersécurité devrait traiter, au moins, des éléments clés mentionnés précédemment, ainsi que de tout autre élément applicable aux activités des sociétés selon leur nature et la taille de la société.*
- *Les sociétés devraient offrir une formation sur la cybersécurité au moins annuellement et suffisamment souvent pour demeurer à jour (plus d'une séance par année peut être nécessaire).*
- *Les sociétés devraient envisager de soumettre régulièrement les employés à des simulations pour évaluer leur capacité à reconnaître et à signaler des activités suspectes, et de fournir de la formation ciblée dans les cas qui ne répondent pas aux attentes.*
- *Si la formation sur la cybersécurité est externalisée à un tiers fournisseur de services, désigner un ou plusieurs membres de la société pour en assurer la supervision afin qu'elle cadre avec ses activités.*
- *Les sociétés devraient tenir des dossiers démontrant que la formation sur la cybersécurité a eu lieu et renfermant le nom des participants, la date de la formation et les éléments abordés.*

3. Évaluation du risque lié à la cybersécurité et contrôles

Si plusieurs sociétés ont mené des évaluations exhaustives du risque lié à la cybersécurité annuellement ou plus souvent (par exemple, trimestriellement ou semestriellement), le personnel a néanmoins constaté que les évaluations d'un certain nombre de sociétés auraient pu être plus rigoureuses, notamment celles qui ne traitaient pas adéquatement des éléments clés ou qui ne faisaient pas l'objet d'une documentation suffisante.

Le personnel a fait les constatations suivantes :

- pendant la période visée par les inspections, les évaluations du risque lié à la cybersécurité auraient pu être plus rigoureuses chez 45 % des sociétés;
- s'agissant des évaluations effectuées au cours de cette période, 12 % des sociétés ne disposaient d'aucune documentation, et bon nombre de sociétés auraient pu améliorer leur documentation en la matière.

De façon générale, le personnel juge que les évaluations du risque lié à la cybersécurité des sociétés, ou la documentation s'y rapportant, pourraient être plus solides dans les cas où elles n'abordaient pas les éléments clés ayant trait à leurs activités. Il s'est appuyé sur les indications de

2017 pour formuler ses observations (voir l'extrait ci-après). Par exemple, il a constaté qu'un certain nombre de sociétés ne s'étaient pas penchées adéquatement sur les éléments suivants :

1) les secteurs de la société vulnérables aux menaces à la cybersécurité (c'est-à-dire les éléments à risque de la société pouvant inclure, globalement, ses appareils, ses données, son courrier électronique, ses sites Web et ses applications);
2) la façon dont les menaces à la cybersécurité et les vulnérabilités sont relevées;
3) les conséquences possibles des différents types de menaces à la cybersécurité qui ont été signalés;
4) l'adéquation des contrôles préventifs de la société aux secteurs à risque.

Extrait des indications de 2017

Les sociétés inscrites devraient, au moins une fois par année, procéder à une évaluation des risques liés à la cybersécurité qui inclurait ce qui suit :

- un inventaire des actifs essentiels et des données confidentielles de la société, notamment les éléments devant être hébergés sur le réseau de la société ou connectés à celui-ci ainsi que les plus importants à protéger;
- les secteurs d'activité de la société qui sont vulnérables aux cybermenaces, notamment les vulnérabilités internes (par exemple, les employés) et externes (par exemple, les pirates et les tiers fournisseurs de services);
- la façon dont les cybermenaces et les vulnérabilités sont relevées;
- les conséquences possibles des différents types de cybermenaces relevés;
- l'adéquation des contrôles préventifs et des plans d'intervention en cas d'incident de la société, notamment l'évaluation des changements à y apporter, s'il y a lieu.

Les sociétés sont invitées à consigner en dossier leurs évaluations du risque, y compris les contrôles qui y sont associés. Le personnel s'attend à ce que la documentation démontre que la société a examiné les éléments ci-dessus de manière appropriée.

En outre, le personnel a relevé des déficiences dans l'évaluation du risque lié à la cybersécurité surtout lorsque 1) les droits d'accès des employés ne constituaient pas un élément de risque, et 2) la société s'en remettait seulement à des tiers fournisseurs de services pour effectuer les évaluations, comme indiqué ci-après.

1) Droits d'accès des employés

   Le personnel a constaté une déficience dans les cas où les droits d'accès des employés (c'est-à-dire l'accès d'un employé notamment aux systèmes et aux données de la société) n'étaient pas caractérisés comme un élément de risque, et que la société n'atténuait pas ce risque au moyen de contrôles adéquats dans son évaluation du risque lié à la cybersécurité.

Voici quelques exemples de contrôles efficaces du risque lié aux droits d'accès des employés que le personnel a observés :

- des contrôles d'accès par fonction, selon lesquels l'accès de l'employé aux systèmes et aux données est associé aux fonctions qui lui sont attribuées (par exemple, par le service des ressources humaines); en cas de mutation ou de départ de l'employé, les droits d'accès sont actualisés ou retirés dans un certain délai; de plus, dans l'attribution de droits à une fonction donnée, il peut être efficace d'envisager l'application du « principe de droit d'accès minimal », qui veut que les employés ne se voient attribuer que le niveau d'accès nécessaire à leurs tâches, sans plus;

- des mesures de surveillance des droits d'accès, notamment l'obligation pour un directeur d'effectuer un examen ou de donner son approbation, s'il y a lieu, et de réviser périodiquement les droits d'accès de tous les employés, particulièrement dans les grandes sociétés où les effectifs sont plus nombreux, pour vérifier si les accès demeurent appropriés.

S'agissant des droits d'accès, le personnel a relevé des déficiences dans les cas où les contrôles avaient été conçus, mais n'étaient pas soutenus par des mécanismes de surveillance et de détection efficaces. Les sociétés devraient déterminer si leurs contrôles de cybersécurité permettent réellement, et en temps utile, de détecter les accès ou les activités non autorisés et d'y répondre.

2) Recours aux tiers fournisseurs de services

Le personnel a observé que certaines sociétés avaient recours à des tiers fournisseurs de services pour mener leurs évaluations du risque lié à la cybersécurité en leur nom et leur fournir un résumé des résultats (par exemple, mettre en relief les secteurs à risque élevé lorsque les contrôles en place étaient inadéquats ou absents). Cette pratique ne pose aucun problème aux yeux du personnel, mais il s'attend à ce que les sociétés :

a) examinent l'évaluation préparée par le tiers fournisseur de services;
b) déterminent l'adéquation de l'évaluation et ajoutent tout élément manquant;
c) décident du traitement à réserver aux préoccupations en matière de cybersécurité relevées par le tiers fournisseur de services.

Le personnel a relevé une déficience dans les cas où la société ne disposait d'aucune documentation attestant qu'elle avait effectué l'examen susmentionné.

Le personnel a remarqué que certaines sociétés faisant appel à des tiers fournisseurs de services pour les aider à évaluer le risque lié à la cybersécurité arrivaient à effectuer pareilles évaluations plus d'une fois par année, ce qui pourrait renforcer leur régime de cybersécurité.

Le personnel a constaté que des sociétés ont adopté une pratique complémentaire efficace qui consistait à faire appel à des tiers fournisseurs de services non seulement pour évaluer le risque lié à la cybersécurité, mais aussi pour effectuer des audits de cybersécurité et des tests d'intrusion. Bien qu'il ne s'agisse pas d'une obligation, le recours à un tiers fournisseur de services pour faire un examen ou simuler une cyberattaque afin de mettre à l'épreuve le régime de cybersécurité de la société peut se révéler efficace pour déceler les vulnérabilités et les lacunes possibles des contrôles. Le personnel a observé un cas où la société recrutait chaque fois un nouveau fournisseur de services pour évaluer les cyberrisques, ce qui lui procurait une diversité de points de vue sur les vulnérabilités possibles.

Contrôles généraux à envisager pour atténuer les éléments de risque

Le personnel s'attend à ce que les sociétés mettent en place des contrôles pour atténuer les éléments de risque mentionnés dans leurs évaluations du risque lié à la cybersécurité. Elles devraient définir les contrôles qui sont mis en œuvre, ou qui le seront, à cette fin, et en évaluer l'adéquation, dans la documentation relative à ces évaluations.

Le personnel fait ressortir ci-après divers contrôles de base que les sociétés devraient envisager de mettre en place afin de prévenir, de détecter et d'atténuer les risques liés à la cybersécurité, si ce n'est déjà fait. *La liste ci-dessous n'est pas exhaustive et a pour but d'aider les sociétés à se donner des moyens de rehausser leur régime de cybersécurité.*

- Exiger des mots de passe complexes (avec des critères de nombre et de type de caractères, de fréquence de renouvellement, etc.).
- Utiliser l'authentification multifactorielle pour ajouter une étape de vérification au-delà du mot de passe, avant la connexion aux systèmes de la société.
- Recourir à des réseaux privés virtuels (RPV; en anglais, *VPN*) pour sécuriser la connexion à distance aux systèmes de la société.
- Chiffrer les données (en transit et stockées) pour protéger les renseignements sensibles contre l'accès et la diffusion non autorisés.
- Maintenir des sauvegardes programmées du système dont la fréquence, la conservation et les tests font l'objet de procédures établies pour assurer la récupérabilité.
- Employer des outils de sécurité (c'est-à-dire des pare-feu et la sécurité des terminaux) pour empêcher les accès non autorisés aux systèmes de la société.
- Filtrer les courriels pour bloquer les pourriels, les tentatives d'hameçonnage et les pièces jointes malveillantes avant qu'ils n'atteignent les utilisateurs.

- Effectuer régulièrement des correctifs et des mises à jour logicielles pour s'attaquer aux vulnérabilités touchant la sécurité en temps opportun.
- Supprimer les logiciels ou applications superflus des appareils de la société afin de réduire l'exposition aux risques liés à la cybersécurité.
- Tenir un registre des activités numériques suspectes pour assurer une vigie des incidents de cybersécurité possibles.
- Supprimer de façon sécuritaire les données sensibles avant l'élimination ou la réutilisation du matériel.

Principaux éléments à retenir pour les sociétés

- *Les sociétés devraient effectuer des évaluations du risque lié à la cybersécurité au moins annuellement, et celles-ci devraient couvrir, à tout le moins, les éléments clés énoncés précédemment ainsi que tout autre élément applicable à leurs activités selon leur nature et la taille de la société.*
- *Le détail de l'évaluation du risque lié à la cybersécurité devrait être consigné en dossier, et celui-ci devrait inclure les contrôles en place pour atténuer les éléments de risque de la société ainsi qu'une évaluation de l'adéquation de ces contrôles.*
- *Si un tiers fournisseur de services effectue l'évaluation du risque lié à la cybersécurité d'une société, ou qu'il y participe, celle-ci devrait consigner en dossier le fait qu'elle a) a examiné l'évaluation menée par le tiers, b) a évalué son adéquation et ajouté les éléments manquants, et c) a répondu aux préoccupations relevées, ou a un plan en vue de le faire.*

4. Tiers fournisseurs de services

Toutes les sociétés inspectées faisaient appel à des tiers fournisseurs de services qui avaient accès à leurs systèmes ou données, y compris des fournisseurs de services infonuagiques pour stocker leurs données et celles de leurs clients.

Le personnel est au fait d'incidents de cybersécurité survenus chez des tiers fournisseurs de services qui étaient engagés par des sociétés inscrites et avaient accès à leurs données confidentielles. Bien que ces types d'incidents ne constituaient pas une intrusion dans les systèmes de la société inscrite, ils pourraient compromettre l'information confidentielle qu'elle détient, y compris les renseignements personnels des clients, de la même façon que si l'incident se produisait au sein de la société.

Par conséquent, il importe que les sociétés perçoivent le recours aux tiers fournisseurs de services comme un élément de risque dans leurs évaluations du risque lié à la cybersécurité. Elles devraient établir et consigner en dossier des contrôles appropriés pour atténuer ce risque.

Comme précisé dans les indications de 2017 (voir l'extrait ci-après), les sociétés devraient effectuer initialement, puis de façon continue, un contrôle diligent suffisant de la cybersécurité de

leurs tiers fournisseurs de services actuels et éventuels, respectivement, et en consigner le détail en dossier. Dans le cadre de ses inspections, le personnel a constaté ce qui suit :

- 41 % des sociétés pourraient renforcer leur surveillance de la cybersécurité des tiers fournisseurs des services.
- 62 % des sociétés ont peu de documentation, voire aucune, étayant cette surveillance.

Extrait des indications de 2017

Les sociétés devraient évaluer périodiquement l'adéquation de leurs pratiques en matière de cybersécurité, notamment les mesures de protection contre les cyberincidents et leur traitement par des tiers ayant accès à leurs systèmes et à leurs données. Elles devraient par ailleurs limiter cet accès.

Contrôle diligent approprié visant les tiers fournisseurs de services

Le personnel s'attend à ce que les sociétés effectuent un contrôle diligent approprié des pratiques de cybersécurité de leurs tiers fournisseurs de services, et en consignent le détail en dossier, pour s'assurer que ces pratiques sont adéquates. Il convient de procéder au contrôle diligent avant d'intégrer un fournisseur, et à une fréquence suffisante pendant toute la durée de la relation.

De l'avis du personnel, il s'agit notamment d'effectuer et de consigner un contrôle diligent adéquat des pratiques de cybersécurité des sociétés technologiques, y compris les bien connues et établies, auxquelles fait appel la société inscrite pour lui fournir des services technologiques tels que de courriel professionnel ou commercial, de gestion documentaire ou encore d'infrastructure. Cependant, le niveau de contrôle diligent nécessaire peut varier en fonction de la nature du fournisseur de services. Par exemple, la société devrait soumettre à un contrôle diligent plus détaillé les fournisseurs de services essentiels à ses activités (par exemple, un comptable, un fournisseur d'information aux clients, un agent des transferts, etc.).

Collecte d'information dans le processus de contrôle diligent

Dans le cadre de son processus de contrôle diligent visant les tiers fournisseurs de services, les sociétés pourraient envisager de recueillir auprès d'eux de l'information relative aux éléments suivants :

- les politiques et procédures de cybersécurité, y compris leur adhésion à des normes de cybersécurité reconnues;
- les pratiques en matière de traitement des données (y compris l'emplacement où les données sont stockées, la méthode de stockage utilisée ainsi que le chiffrement des données stockées et en transit);
- les emplacements physique et légal où sont exercées leurs activités, les obligations qui leur sont applicables dans leur territoire ainsi que tous les risques pouvant en découler;

- les contrôles des accès;
- les processus de gestion des vulnérabilités et des correctifs;
- les pratiques en matière de sécurité physique;
- les protocoles de détection et d'intervention en cas d'incident de cybersécurité, y compris le moyen par lequel la société serait informée si elle avait été touchée, et le moment auquel elle le serait;
- la gestion des incidents de cybersécurité passés;
- la gestion de leurs tiers fournisseurs de services;
- la fréquence des évaluations du risque lié à la cybersécurité (par exemple, régulièrement);
- les attentes de séparation des responsabilités à l'égard de la sécurité entre le fournisseur de services et la société, de manière à définir clairement la responsabilité de la protection des systèmes et des données dans un environnement infonuagique partagé.

Pratiques de contrôle diligent observées

Voici des exemples de pratiques observées que les sociétés pourraient envisager de mettre en place dans leur contrôle diligent de cybersécurité visant les tiers fournisseurs de services :

- faire remplir au tiers fournisseur de services un questionnaire sur la cybersécurité lors de son recrutement, et actualiser les réponses fournies selon une fréquence appropriée (par exemple, annuellement) pendant la durée de la relation;
- obtenir du tiers fournisseur de services une attestation concernant les modalités de protection des systèmes et des données de la société inscrite;
- tenir à jour un registre de l'ensemble des tiers fournisseurs de services et la documentation à l'appui du contrôle diligent;
- recevoir et examiner périodiquement des rapports des tiers fournisseurs de services sur la cybersécurité.

Les inspections ont relevé ce qui suit au sujet des sociétés recevant de tels rapports :

- les rapports étaient la plupart du temps reçus et examinés annuellement;
- les rapports les plus fréquemment reçus et examinés étaient ceux sur les contrôles des sociétés de services (**rapports SOC**). En particulier, les rapports SOC 2 présentent une évaluation des contrôles de sécurité de la société concernée, et sont habituellement produits annuellement; dans le cadre du contrôle diligent initial ou continu mené sur le tiers fournisseur de services, il est conseillé de demander pour examen un rapport SOC 2 récent ou un rapport similaire, s'il est disponible;
- la reddition de comptes prenait également d'autres formes, notamment les suivantes :
    - un questionnaire à jour de contrôle diligent de la cybersécurité du fournisseur de services;
    - une évaluation récente du risque lié à la cybersécurité du fournisseur de services;

- le plan d'intervention actuel en cas d'incident de cybersécurité du fournisseur de services.

Principaux éléments à retenir pour les sociétés

- *Les sociétés devraient effectuer un contrôle diligent approprié des pratiques de cybersécurité des tiers fournisseurs de services pour s'assurer qu'elles sont adéquates. Ce contrôle devrait être fait avant l'intégration du tiers fournisseur de services, et à une fréquence appropriée pendant toute la durée de la relation.*
- *Les sociétés devraient tenir à jour une documentation adéquate démontrant que les tiers fournisseurs de services ont fait l'objet d'un contrôle diligent de la cybersécurité.*

5. Plan d'intervention en cas d'incident de cybersécurité

Le personnel a constaté que certaines sociétés avaient défini par écrit ce qu'est un « incident de cybersécurité », et d'autres, non. À son avis, formuler une définition est une première étape importante en vue d'élaborer un plan d'intervention efficace en cas d'incident de sécurité (un **plan d'intervention**), car la définition éclaire sur le moment auquel celui-ci devrait être déclenché.

De manière générale, chez les sociétés où il en existait une, la définition d'« incident de cybersécurité » incluait les éléments suivants :

- un événement pouvant compromettre la confidentialité, l'intégrité ou la disponibilité des systèmes, des données ou des services de la société;
- un événement entraînant, ou pouvant entraîner, la divulgation non autorisée de renseignements sensibles, comme de l'information d'identification personnelle, de l'information financière ou des dossiers de la société portant sur des personnes physiques ou des tiers fournisseurs de services;
- tout accès ou tentative d'accès non autorisé aux systèmes de la société;
- un événement accidentel ou délibéré qui touche les systèmes et les données de la société (y compris toute utilisation abusive, perte, divulgation, destruction, modification ou tout vol);
- un événement pouvant occasionner un préjudice ou des inconvénients aux clients, et menacer de perte ou de perturbation les activités, la réputation ou les actifs de l'entreprise;
- un événement que l'on a déterminé comme ayant une incidence sur la société et qui nécessitera une intervention et des mesures de reprise.

Le personnel a fait les constatations suivantes :

- 15 % des sociétés ne disposaient d'aucun plan d'intervention écrit;
- 53 % des sociétés s'étant doté d'un tel plan auraient pu le renforcer davantage;

- 63 % des sociétés qui disposaient d'un plan d'intervention écrit devraient le mettre à l'essai plus régulièrement.

Voici les indications publiées antérieurement sur les plans d'intervention écrits, les sauvegardes de données et l'assurance cybersécurité :

Extrait des indications de 2017

Les sociétés devraient établir par écrit un plan d'intervention en cas de cyberincident pour répondre à un tel incident et le signaler. Ce plan devrait prévoir ce qui suit :

- les personnes chargées de communiquer le cyberincident et celles participant à la réponse;
- la description des différents types de cyberattaques (par exemple, des infections par maliciel, des menaces internes, des virements de fonds frauduleux par Internet) auxquels la société est exposée;
- les procédures visant à ce que l'incident cesse de causer des dommages et à éradiquer ou neutraliser la menace;
- les procédures relatives à la récupération des données;
- la réalisation d'une enquête sur l'incident afin d'établir la portée des dommages et en trouver la cause, de sorte que les systèmes de la société puissent être modifiés pour empêcher un autre incident semblable;
- l'identification des parties devant être avisées et de l'information devant être communiquée.

…

Nous nous attendons à ce que les sociétés sauvegardent leurs données et soumettent régulièrement leurs processus de sauvegarde à des essais

…

Les sociétés devraient revoir leurs polices d'assurance actuelles (par exemple, les assurances d'institution financière) pour connaître les types de cyberincidents couverts. Elles devraient envisager de souscrire une assurance supplémentaire si des éléments ne sont pas couverts par leurs polices actuelles.

…

Quelle que soit sa taille ou les fonctions imparties, toute société devrait se doter de politiques et de procédures relatives à la cybersécurité et, en particulier, d'un plan d'intervention en cas de cyberincident régulièrement soumis à des essais.

17

Élaboration d'un plan d'intervention

De manière générale, le personnel a observé que le plan d'intervention écrit des sociétés pourrait être rehaussé dans les cas où celui-ci n'abordait pas certains éléments clés d'un plan efficace. Il s'est appuyé sur les indications de 2017 pour formuler ses observations (voir l'extrait ci-dessus). Par exemple, il a conclu que le plan d'intervention écrit de plusieurs sociétés ne décrivait pas les différents types de cyberattaques pouvant être lancées contre elles.

Les incidents de cybersécurité chez un tiers fournisseur de services ayant accès aux systèmes ou aux données de la société peuvent avoir sur les renseignements confidentiels de cette dernière des répercussions qui sont identiques ou semblables à celles d'un incident chez la société inscrite elle-même. Ainsi, le personnel a également constaté que le plan d'intervention écrit d'une société pourrait être davantage renforcé en y incluant des procédures d'intervention en cas d'incident de cybersécurité chez un tiers fournisseur de services qui a accès à ses systèmes et à ses données. Il s'attend à ce que la société y prévoie sa réponse si elle est informée d'un tel incident.

Sauvegarde et récupération des données

Le personnel a relevé des déficiences chez les sociétés qui ne mettaient pas à l'essai régulièrement la sauvegarde des données ou ne tenaient pas de dossiers de ces essais. Les sociétés appliquant des pratiques prudentes de cybersécurité devraient se demander si elles sont munies des dispositifs de sauvegarde nécessaires en fonction de leur taille et de leur complexité, mettre à l'essai régulièrement la sauvegarde ainsi que la récupération, et consigner en dossier le détail de ces essais ainsi que leur capacité à récupérer leurs données rapidement.

Assurance cybersécurité

Les sociétés ont répondu, dans une proportion de 62 %, avoir souscrit une police d'assurance cybersécurité. En outre, certaines sociétés qui n'avaient pas de polices d'assurance cybersécurité distinctes ont indiqué que les incidents de cybersécurité étaient couverts en vertu d'autres polices d'assurance.

Même si la souscription d'une assurance cybersécurité n'est pas obligatoire, le personnel est d'avis qu'elle peut être avantageuse, car elle permet d'amoindrir le préjudice financier susceptible de découler d'un incident de cybersécurité. De plus, les processus de l'assureur ainsi que son assistance opérationnelle peuvent aider dans la résolution de l'incident de cybersécurité (par exemple, aider à engager des avocats spécialisés en incidents de cybersécurité ou d'autres spécialistes qualifiés, au besoin).

Mise à l'essai des plans d'intervention

Compte tenu des défis persistants que posent les menaces à la cybersécurité et de leur évolution rapide, le personnel s'attend, comme le précisent les indications de 2017, à ce que les sociétés mettent à l'essai régulièrement leur plan d'intervention. Il devrait y avoir de la documentation étayant ces essais.

La mise à l'essai du plan d'intervention est importante, car elle permet aux sociétés, et surtout aux équipes et aux personnes concernées, d'être prêtes à intervenir de façon efficace et efficiente lors de tout incident de cybersécurité. Elle peut aider les personnes clés à mieux se préparer à un incident réel, et les sociétés à cerner les lacunes potentielles à corriger dans leur plan d'intervention.

Les sociétés peuvent mettre à l'essai leur plan d'intervention de diverses façons, y compris les suivantes :

- **Exercices sur table** : Tests de cheminement prenant la forme d'une discussion sur des scénarios hypothétiques d'incidents de cybersécurité. Les personnes clés prenant part à l'intervention discutent des différentes étapes figurant dans le plan d'intervention. L'adéquation de ce plan peut ainsi être évaluée.
- **Simulations d'attaque :** Exercices de cybersécurité pratiques et techniques au cours desquels deux équipes, l'une représentant les pirates, et l'autre, les défenseurs, travaillent ensemble pour déterminer à quel point la société et ses systèmes arrivent à détecter des cybermenaces réelles, et à y répondre. Ils permettent d'évaluer le fonctionnement des contrôles techniques de cybersécurité ainsi que l'adéquation du plan d'intervention.

Ces essais peuvent être menés à l'interne ou avec l'aide de tiers fournisseurs de services.

Principaux éléments à retenir pour les sociétés

- *Les sociétés devraient disposer d'un plan d'intervention écrit exhaustif qui aborde, à tout le moins, les principaux éléments indiqués ci-dessus, ainsi que tout autre élément applicable aux activités de la société selon leur nature et la taille de celle-ci.*
- *Les sociétés devraient procéder à la sauvegarde de leurs données et mettre à l'essai régulièrement leur procédure de récupération. Elles devraient consigner en dossier le détail de ces essais ainsi que leur capacité à récupérer leurs données rapidement.*
- *Les sociétés devraient mettre à l'essai régulièrement leur plan d'intervention et tenir une documentation étayant ces essais.*

QUESTIONS

Pour toute question, veuillez vous adresser aux membres du personnel suivants :

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

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 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
Agente de conformité, Division des valeurs mobilières
Commission des services financiers et des services aux consommateurs du Nouveau-Brunswick
506 721-5223
michelle.doucette@fcnb.ca

Aishah Abdullahi
Compliance Auditor
Commission des valeurs mobilières du Manitoba
204 945-8973
aishah.abdullahi@gov.mb.ca

Angela Duong
Deputy Director, Compliance and Oversight
Commission des valeurs mobilières du Manitoba
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
Commission des valeurs mobilières de l'Ontario
416 597-7230
scardinale@osc.ca

Alizeh Khorasanee
Head of Dealer Compliance, Registration, Inspections and Examinations
Commission des valeurs mobilières de l'Ontario
416 716-3307
akhorasanee@osc.ca

Susan Pawelek
Senior Accountant, Registration, Inspections and Examinations
Commission des valeurs mobilières de l'Ontario
416 593-3680
spawelek@osc.ca