CSA/ACVM Canadian Securities Administrators | Autorités canadiennes en valeurs mobilières

Avis 33-321 du personnel des ACVM
Cybersécurité et médias sociaux

Le 19 octobre 2017

Introduction

Le personnel des Autorités canadiennes en valeurs mobilières (le **personnel des ACVM** ou **nous**) a mené, du 11 octobre au 4 novembre 2016, un sondage sur les pratiques en matière de cybersécurité et de médias sociaux. Les cybermenaces et les médias sociaux sont des risques auxquels les sociétés inscrites sont de plus en plus exposées. Il s'agit de risques complexes, en constante évolution et généralisés. Le sondage visait à recueillir de l'information auprès des sociétés inscrites à titre de gestionnaires de fonds d'investissement, de gestionnaires de portefeuille et de courtiers sur le marché dispensé, à cerner les tendances et à établir la base des indications à fournir au sujet des pratiques en matière de cybersécurité et de médias sociaux.

Conformément à 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**), la société inscrite doit établir, maintenir et appliquer des politiques et des procédures instaurant un système de contrôles et de supervision capable de garantir la conformité à la législation en valeurs mobilières et de gérer les risques liés à son activité conformément aux pratiques commerciales prudentes. Ces systèmes de conformité devraient encadrer les risques liés aux cybermenaces et l'utilisation des médias sociaux, qui posent tous deux des risques pour l'ensemble des sociétés inscrites. Dans l'Avis 11-332 du personnel des ACVM, *Cybersécurité*, précédemment publié, nous soulignions l'importance d'atténuer les cyberrisques et avons précisé que nous nous attendions à ce que les sociétés inscrites fassent preuve de vigilance lors de l'élaboration, de la mise en œuvre et de l'actualisation des mesures appropriées pour se protéger, ainsi que leurs clients, contre les cybermenaces. Nous indiquions également que, dans le cadre des examens de la conformité, nous allions échanger avec les sociétés inscrites au sujet des politiques et procédures relatives à la cybersécurité.

Comme l'indiquait l'Avis 31-325 du personnel des ACVM, *Pratiques de commercialisation des gestionnaires de portefeuille* (l'**Avis 31-325 du personnel des ACVM**), l'utilisation des médias sociaux comme moyen de communication avec la clientèle et le public pose des défis sur le plan de la conformité et de la supervision pour les sociétés, notamment un risque accru que les sociétés inscrites utilisant ces plateformes ne tiennent pas de dossiers adéquats de leurs activités commerciales et de leurs communications avec les clients. L'article 11.5 du Règlement 31-103 oblige la société inscrite à consigner avec exactitude ses activités commerciales, ses affaires financières et les opérations de ses clients dans ses dossiers.

Par ailleurs, les sociétés devraient prendre en considération les cyberrisques associés à l'utilisation des médias sociaux. Des pirates informatiques pourraient, par exemple, utiliser l'information affichée sur les sites de médias sociaux à des fins commerciales ou personnelles pour s'infiltrer dans leurs systèmes et obtenir de l'information confidentielle.

En plus d'exposer les résultats du sondage, le présent avis vise à fournir aux sociétés des indications plus précises en proposant des politiques et des procédures sur les pratiques en

matière de cybersécurité et de médias sociaux. Toutes les sociétés inscrites devraient adopter de telles pratiques, qui doivent inclure des mesures préventives, la formation de tous les employés et un plan d'intervention en cas de cyberincident.

Sondage

Le sondage a été envoyé à plus de 1 000 sociétés inscrites, et 63 % d'entre elles y ont répondu.

Les questions du sondage étaient conçues de façon à recueillir de l'information sur les aspects suivants :

- les politiques et procédures de la société sur ses pratiques en matière de cybersécurité et de médias sociaux, notamment les renseignements au sujet de la personne qui en est responsable et de la formation offerte à ses employés;

- l'évaluation des risques effectuée par la société pour cerner les cybermenaces, les vulnérabilités et les conséquences possibles;

- les cyberincidents dont la société a été l'objet;

- le plan d'intervention de la société en cas de cyberincident;

- le contrôle diligent effectué par la société pour évaluer les pratiques de cybersécurité des tiers fournisseurs, des consultants ou d'autres fournisseurs de services;

- les politiques et les procédures de chiffrement des données ou des systèmes de la société et ses processus de sauvegarde;

- la façon dont la société surveille ses activités sur les médias sociaux, notamment ses lignes directrices en matière de contenu et de tenue de dossiers appropriés.

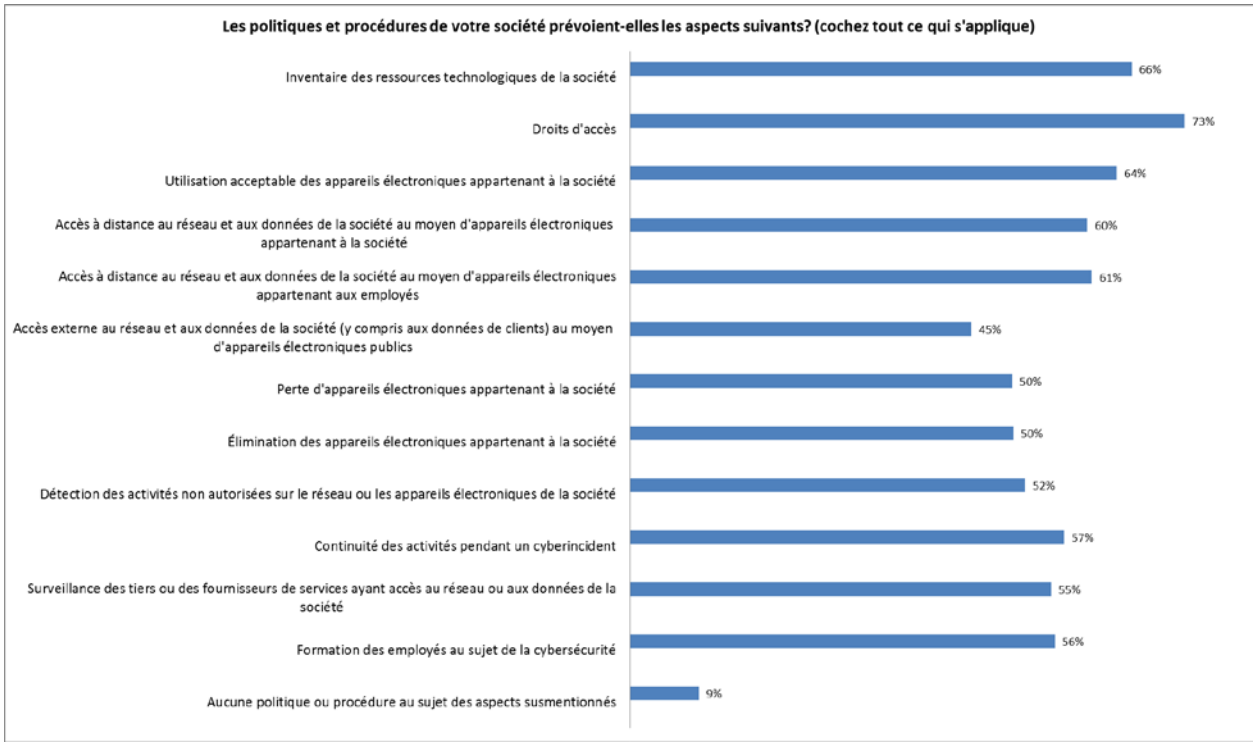
Résumé des résultats du sondage et indications

A. Cybersécurité

Environ 51 % des sociétés ont été l'objet d'un cyberincident au cours de l'année sondée. L'hameçonnage, rapporté par 43 % des sociétés, est le plus courant, tandis que 18 % ont été la cible de maliciels, et 15 %, d'une tentative frauduleuse de se faire passer, par courriel, pour un client afin de faire transférer ses fonds ou ses valeurs mobilières. L'atténuation des cybermenaces revêt de l'importance dans la capacité d'une société à gérer ses risques.

1. Politiques et procédures

La plupart des sociétés sont dotées de politiques et de procédures traitant de cybersécurité. Or, seulement 57 % des sociétés sondées disposent de politiques et de procédures précisément liées à la continuité de leurs activités pendant un cyberincident, et uniquement 56 %, de politiques et de procédures relatives à la formation de leurs employés au sujet de la cybersécurité.



Indications :

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;

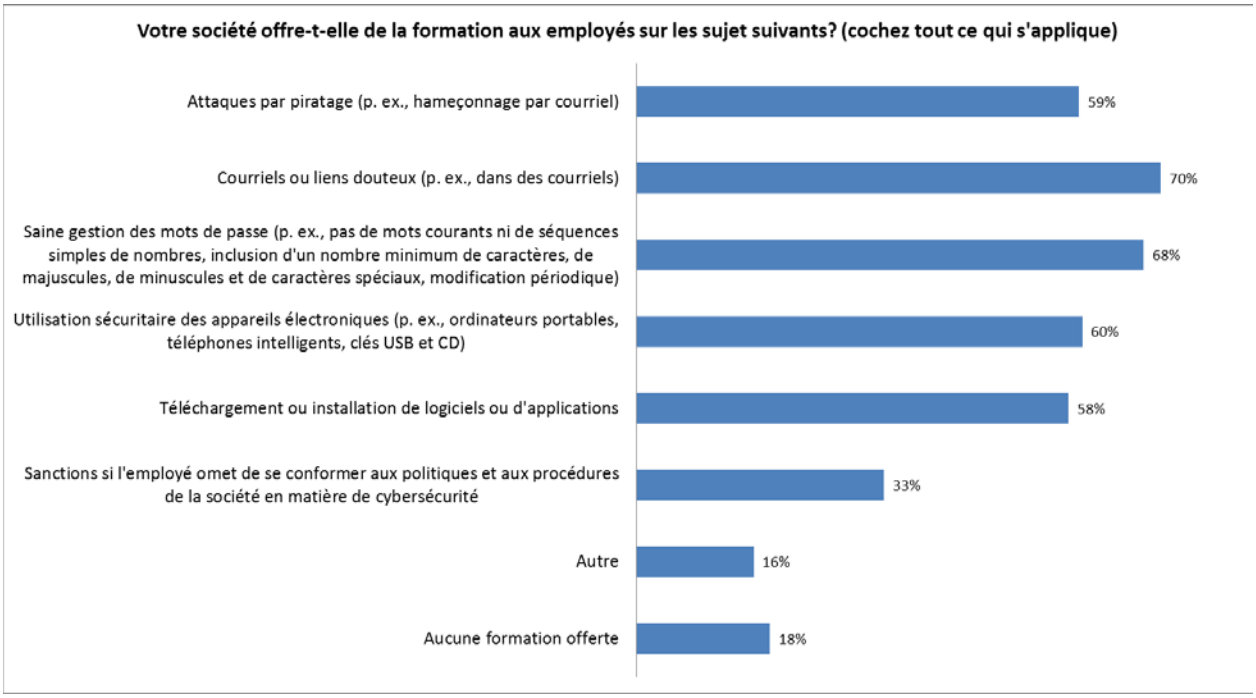
- la supervision des tiers fournisseurs, notamment de services, ayant accès au réseau ou aux données de la société (par exemple, au moyen d'un examen approfondi ou d'une entente de confidentialité);

- la déclaration de tout cyberincident au conseil d'administration (ou son équivalent).

Les politiques et procédures de la société devraient être conçues pour protéger la confidentialité, l'intégrité et la disponibilité de ses données, notamment les renseignements personnels des clients. Pour suivre l'évolution des cybermenaces, la société devrait les revoir et les actualiser régulièrement.

2. Formation

Les sociétés offrant de la formation à leurs employés mettent l'accent sur les courriels ou les liens douteux, les saines pratiques en matière de mot de passe et l'utilisation sécuritaire du matériel ou des logiciels.



Indications :

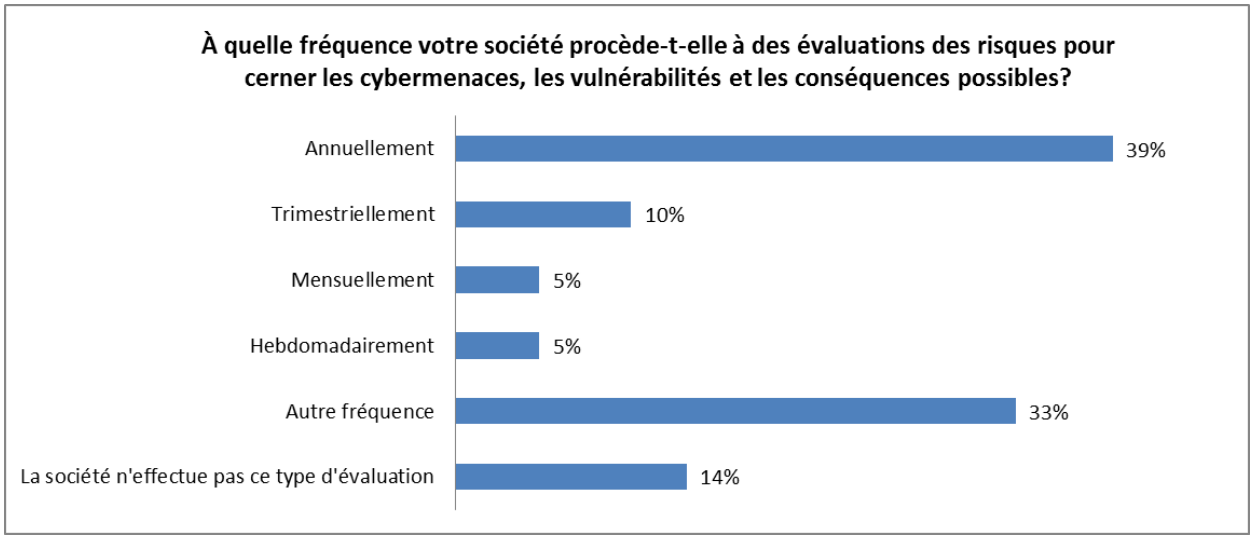
Les employés étant souvent la première ligne de défense lors d'une attaque, la société se doit d'offrir une formation adéquate sur les pratiques en matière de cybersécurité afin de parer à toute cybermenace ou à tout cyberincident. Les employés devraient être informés des risques associés aux données qu'ils peuvent recueillir, utiliser ou divulguer et sur l'utilisation sécuritaire de tous les appareils électroniques. La formation peut être dispensée par la société elle-même ou par l'entremise de tiers.

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.

3. Évaluation des risques

La plupart des sociétés procèdent à une évaluation des risques au moins annuellement pour cerner les cybermenaces. Toutefois, 14 % d'entre elles ont déclaré ne pas le faire.



En réponse à la question ci-dessus, la plupart des sociétés ayant répondu « Autre fréquence » ont indiqué qu'elles évaluaient les risques de façon continue (par exemple, une surveillance continue par un logiciel, un tiers fournisseur de services ou leur société mère) ou, dans certains cas, elles évaluaient les risques à une fréquence différente (par exemple, semestriellement ou au besoin, comme à la suite de changements apportés au matériel ou aux logiciels).

Indications :

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);

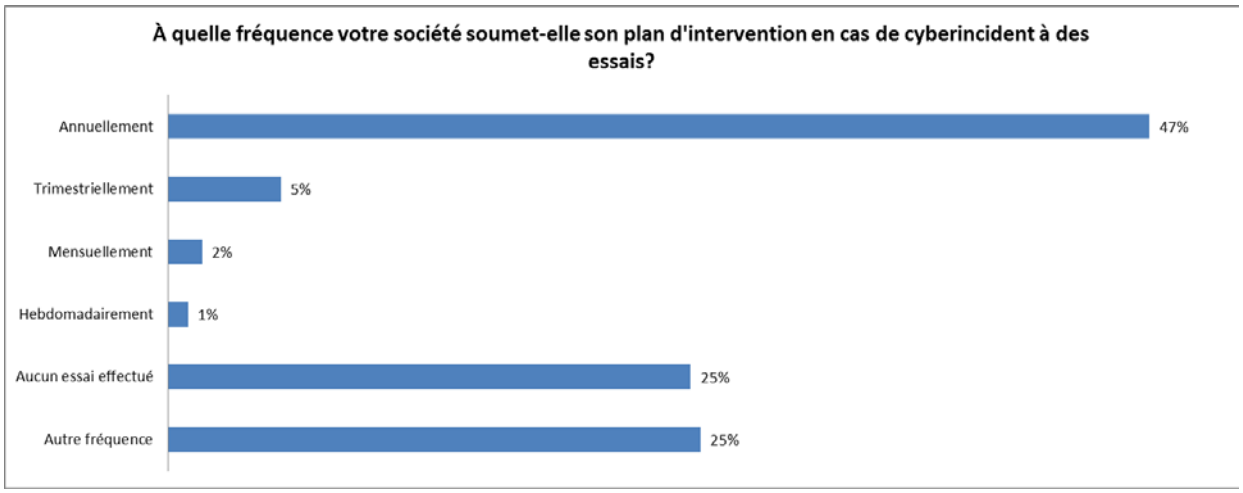
- la façon dont les cybermenaces et les vulnérabilités sont relevées;

- 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.

4. Plan d'intervention en cas d'incident

Un nombre important de sociétés (66 %) ont établi un plan d'intervention en cas de cyberincident qui est soumis à des essais au moins une fois par année. Comme l'indique le tableau ci-dessous, la fréquence des essais peut varier et bon nombre de sociétés n'en effectuent pas.



Les sociétés ayant répondu « Autre fréquence » ont soumis leur plan à une fréquence différente (par exemple, semestriellement, annuellement ou au besoin, comme à la suite d'un changement), ou ont indiqué que leur plan serait soumis à des essais l'année suivante.

Indications :

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;

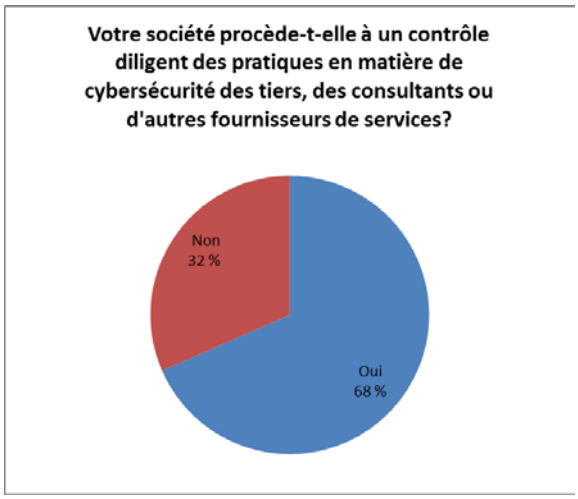
- l'identification des parties devant être avisées et de l'information devant être communiquée.

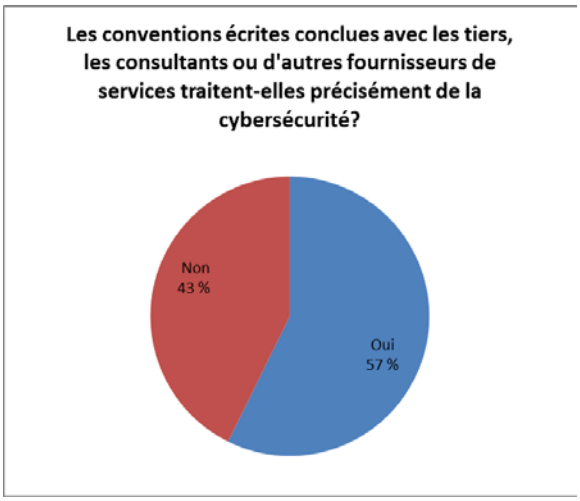
5. Contrôle diligent

Un nombre considérable de sociétés sondées (92 %) ont fait appel à des tiers, des consultants ou à d'autres fournisseurs de services (par exemple, un fournisseur de TI, un dépositaire, un agent chargé de la tenue des registres, un agent des transferts ou un agent d'évaluation). La majorité d'entre elles ont effectué un contrôle diligent des pratiques en matière de cybersécurité de ces tierces parties.

L'ampleur du contrôle diligent effectué et la façon dont il est documenté varient grandement. Certaines sociétés exigent que les tiers leur remettent des exemplaires de leurs politiques et procédures relatives à leurs pratiques de cybersécurité; certaines ajoutent des conditions relatives à la cybersécurité dans leurs conventions écrites; certaines se fient aux normes de diligence concernant la confidentialité ou la protection des données et des renseignements, alors que d'autres s'en remettent simplement à la taille et à la réputation des tiers sans effectuer d'examen approfondi.

La majorité des sociétés ont indiqué que les conventions écrites conclues avec les tiers, les consultants ou les autres fournisseurs de services traitaient précisément de la cybersécurité.





Certaines sociétés ont indiqué que dorénavant, elles allaient procéder à un contrôle diligent et inclure dans leurs conventions écrites des conditions propres à la cybersécurité au fur et à mesure qu'elles les mettent à jour ou dès qu'elles en concluront de nouvelles.

Indications :

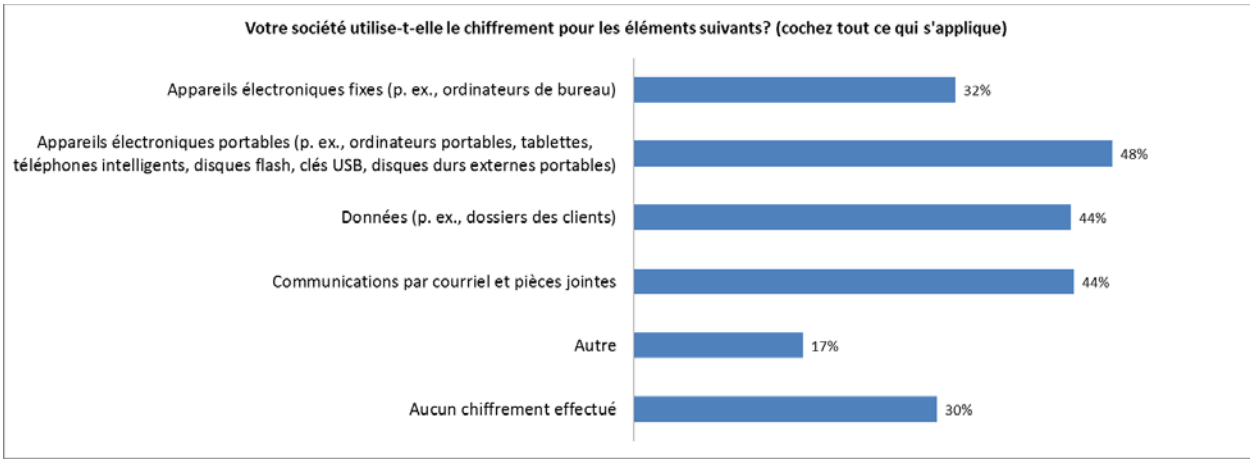
Les sociétés devraient évaluer périodiquement l'adéquation de leurs pratiques en matière de cybersécurité, notamment les mesures de protection contre les cyberincidents et leur traitement par des tiers ayant accès à leurs systèmes et à leurs données. Elles devraient par ailleurs limiter cet accès.

Les conventions écrites conclues avec ces parties externes devraient prévoir des dispositions relatives aux cybermenaces, notamment l'obligation que celles-ci avisent la société de tout cyberincident découlant d'un accès non autorisé à ses réseaux ou à ses données et de leur plan d'intervention pour parer à ces incidents.

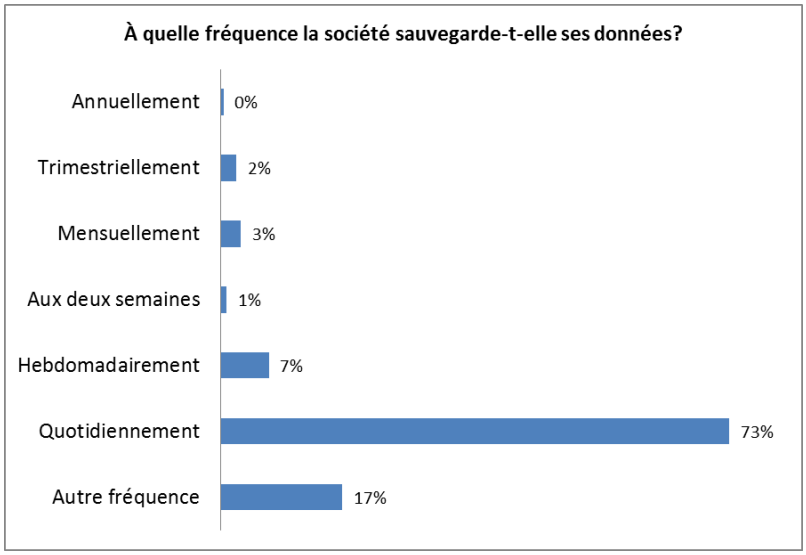
Les sociétés ayant recours à des services infonuagiques devraient comprendre les pratiques en matière de sécurité adoptées par leur fournisseur pour se protéger contre les cybermenaces et déterminer si les pratiques sont adéquates. Elles devraient ainsi établir des procédures si des données en nuage devenaient inaccessibles.

6. Protection des données

Les données de clients peuvent être stockées ou accessibles au moyen de technologies diverses comme le courriel, le stockage infonuagique et les sites Web. Le chiffrement est l'un des outils à la disposition des sociétés pour protéger leurs données et l'information sensible contre les accès non autorisés. Comme l'indiquent les réponses à la question ci-après, un nombre appréciable de sociétés n'utilisent ni le chiffrement ni d'autres mesures de protection des données, comme la protection des documents par mot de passe.



Hormis quatre sociétés, toutes celles sondées ont indiqué qu'elles sauvegardaient leurs données périodiquement. De ces sociétés, 73 % effectuent des sauvegardes quotidiennes et 89 % ont soumis leurs processus de récupération des sauvegardes à des essais.



Certaines sociétés ont répondu « Autre fréquence » parce qu'elles sauvegardent leurs données plusieurs fois par jour (certaines le font même à toutes les heures) ou parce que la fréquence varie selon le type de données (par exemple, les données ou les systèmes jugés essentiels sont sauvegardés toutes les 15 minutes, alors que les données non essentielles sont sauvegardées quotidiennement, hebdomadairement, etc.).

Un nombre important de sociétés permettent à leurs clients et aux tiers (par exemple, les courtiers, les fournisseurs de services) d'accéder à leurs données et à leurs systèmes. En revanche, cet accès ne se fait pas toujours par des canaux sécurisés.

Indications :

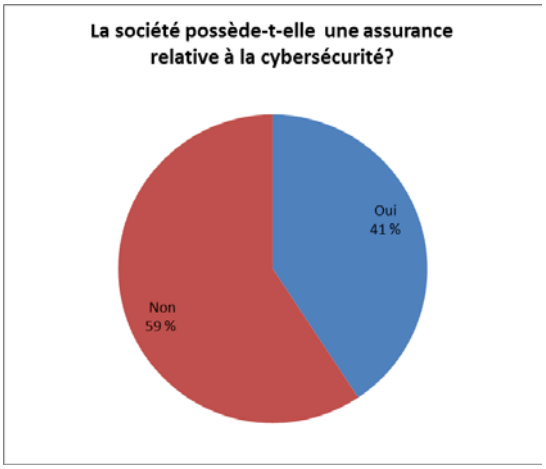
Le chiffrement protège la confidentialité des renseignements puisque seuls les utilisateurs autorisés peuvent consulter les données. Outre le chiffrement pour tous les ordinateurs et autres appareils électroniques, les sociétés devraient imposer l'utilisation de mots de passe pour y accéder. Un mot de passe efficace nécessite différents types de caractères (par exemple, des chiffres, des lettres majuscules et des symboles) et doit être modifié fréquemment.

Les sociétés offrant des portails à leurs clients ou à d'autres tiers à des fins de communications ou pour accéder à leurs données ou leurs systèmes devraient s'assurer que l'accès est sécurisé et que les données sont protégées.

Nous nous attendons à ce que les sociétés sauvegardent leurs données et soumettent régulièrement leurs processus de sauvegarde à des essais. Lors de la sauvegarde des données, elles devraient également veiller à ce que les données soient sauvegardées sur un serveur externe sécurisé advenant des dommages matériels à leurs locaux.

7. Assurance

La majorité des sociétés (59 %) ne détiennent pas d'assurance relative à la cybersécurité. Le type d'incidents et les montants couverts par ces polices varient grandement parmi les sociétés ayant souscrit ce type d'assurance.



Indications :

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.

Autres commentaires

Quelques sociétés de petite taille ou nouvellement inscrites ont précisé qu'elles estimaient que leurs risques liés à la cybersécurité étaient faibles en raison de leur taille. Elles n'ont donc pas senti le besoin d'élaborer de politiques et de procédures relatives à la cybersécurité ou d'offrir de formation à leurs employés. Cependant, le secteur financier est une cible bien connue des cybercriminels. D'autres sociétés ont par ailleurs indiqué qu'elles se fiaient aux mesures de protection instaurées par leur société mère ou leurs fournisseurs de services (par exemple, un dépositaire, un agent des transferts, un fournisseur de services infonuagiques). 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.

Ressources en matière de cybersécurité

L'Avis 11-332 du personnel des ACVM, *Cybersécurité*, présente une liste de documents de référence établis par divers organismes de réglementation et de normalisation qui peuvent être utiles aux sociétés, notamment les suivants :

- *Guide de pratiques exemplaires en matière de cybersécurité* de l'OCRCVM
  http://www.ocrcvm.ca/industry/Documents/CybersecurityBestPracticesGuide_fr.pdf

- *Gestion des cyberincidents – Guide de planification* de l'OCRCVM
  http://www.ocrcvm.ca/industry/Documents/CyberIncidentManagementPlanningGuide_fr.pdf

- Bulletin #0690 de l'Association canadienne des courtiers de fonds mutuels (ACFM)
  http://www.mfda.ca/regulation/bulletins16/Bulletin0690-C_fr.pdf

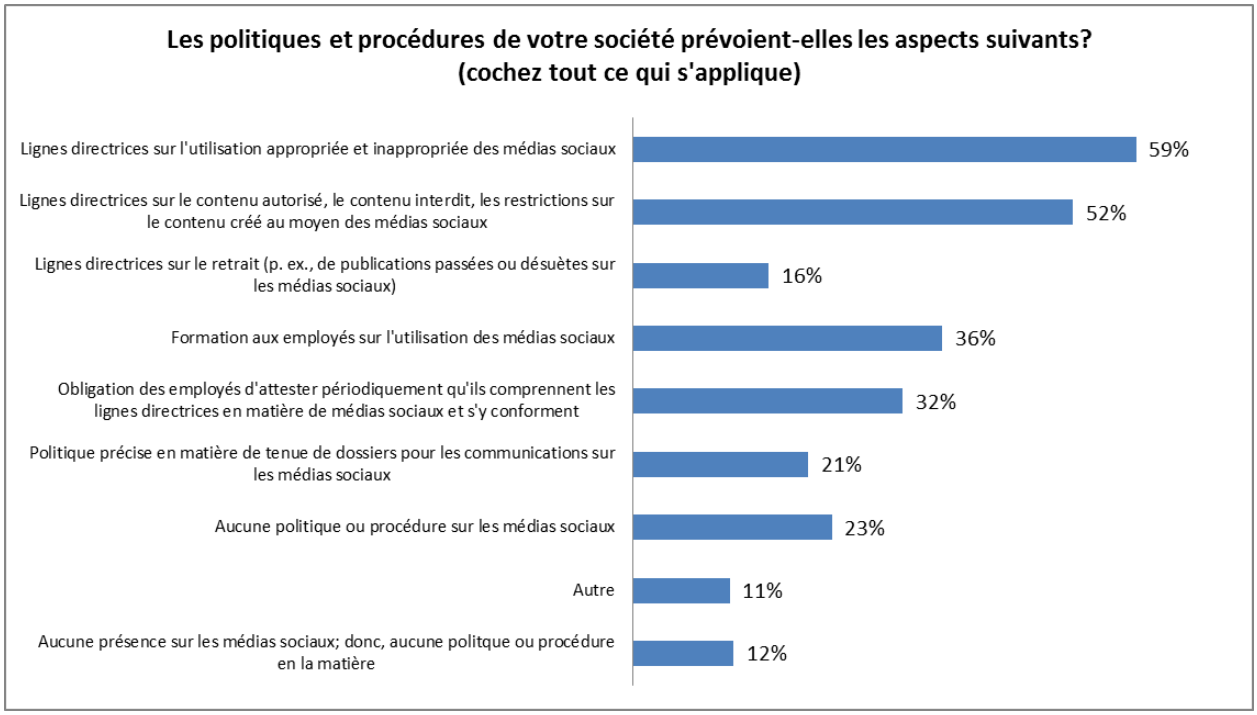
- *Conseils sur l'autoévaluation en matière de cybersécurité* du Bureau du surintendant des institutions financières (BSIF)
  http://www.osfi-bsif.gc.ca/fra/fi-if/in-ai/pages/cbrsk.aspx

B. Médias sociaux

Les médias sociaux peuvent servir à mener une cyberattaque. Par exemple, des pirates peuvent utiliser les sites de médias sociaux pour envoyer un courriel ou un lien d'hameçonnage pouvant mener à des sites Web installant des maliciels. Si les résultats du sondage et les indications présentées ci-après mettent l'accent sur l'utilisation des médias sociaux à des fins de commercialisation, ils devraient également être pris en considération dans le contexte de la cybersécurité.

1. Politiques et procédures

La plupart des sociétés sont dotées de politiques et de procédures sur les pratiques en matière de médias sociaux. Bien que 59 % des sociétés sondées disposent de lignes directrices sur l'utilisation appropriée et inappropriée des médias sociaux, seules 36 % ont établi des politiques et des procédures sur la formation des employés en la matière, et 21 % sont dotées de politiques propres à la tenue de dossiers de communications sur les médias sociaux.



Indications :

Les sociétés devraient revoir, superviser et conserver le contenu sur les médias sociaux et avoir la capacité de l'extraire. Les politiques et les procédures sur les pratiques en matière de médias sociaux devraient inclure ce qui suit :

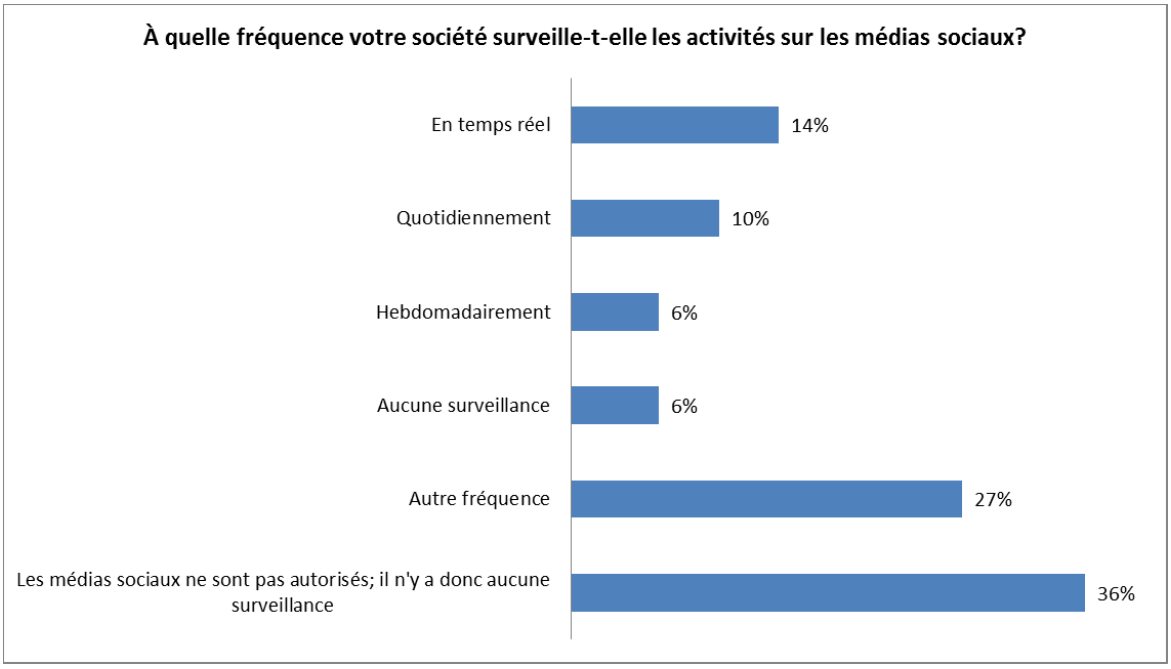
- des lignes directrices sur l'utilisation appropriée des médias sociaux, notamment leur utilisation à des fins commerciales;

- des lignes directrices sur le contenu autorisé sur les médias sociaux;
- des procédures visant à s'assurer que le contenu affiché sur les médias sociaux est à jour;
- des obligations de tenue de dossiers sur le contenu affiché sur les médias sociaux;
- l'examen et l'approbation du contenu affiché sur les médias sociaux, y compris une preuve de ceux-ci.

Les sociétés trouveront davantage d'indications sur les éléments susmentionnés dans l'Avis 31-325 du personnel des ACVM.

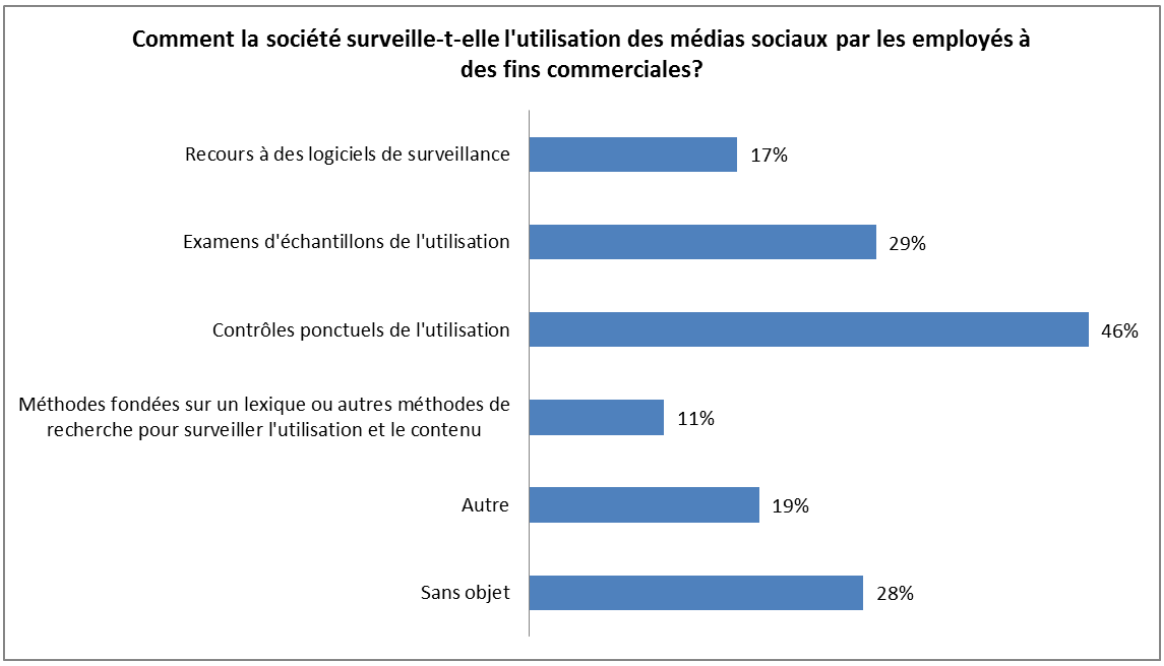
2. Surveillance des activités sur les médias sociaux, notamment leur utilisation par les employés à des fins commerciales et personnelles

Seul un petit pourcentage de sociétés (14 %) surveillent en temps réel les activités sur les médias sociaux. Un pourcentage limité de sociétés (6 %) ne les surveillent aucunement.



Certaines sociétés ayant répondu « Autre fréquence » à la question ci-dessus surveillent les activités sur les médias sociaux de façon annuelle, trimestrielle, mensuelle ou au besoin.

Pour surveiller l'utilisation des médias sociaux par leurs employés à des fins commerciales, 46 % des sociétés effectuent des contrôles ponctuels ou examinent des échantillons.



Indications :

Compte tenu de la facilité avec laquelle l'information peut être affichée sur les plateformes de médias sociaux, de la difficulté à la retirer une fois affichée et de la nécessité de réagir rapidement aux enjeux qu'elle peut soulever, les sociétés devraient se doter de procédures appropriées d'approbation et de surveillance concernant les communications sur les médias sociaux. Même les sociétés ne permettant pas l'utilisation des médias sociaux à des fins commerciales devraient établir des politiques et des procédures pour surveiller toute utilisation non autorisée.

On trouvera des indications supplémentaires sur l'utilisation des médias sociaux dans l'Avis 31-325 du personnel des ACVM.

Prochaines étapes

Nous continuerons d'évaluer les pratiques des sociétés en matière de cybersécurité et de médias sociaux dans le cadre de nos examens de la conformité. Lorsque nous évaluerons si les sociétés s'acquittent de leurs obligations de gestion des risques associés à leurs activités, comme le prévoit le Règlement 31-103, nous appliquerons l'information et les indications figurant dans le présent avis.

Questions

Pour toute question, veuillez vous adresser à l'une des personnes suivantes :

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

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

Angela Duong
Compliance Auditor
Commission des valeurs mobilières du Manitoba
204 945-8973
angela.duong@gov.mb.ca

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

To-Linh Huynh
Senior Analyst
Commission des services financiers et des services
aux consommateurs (Nouveau-Brunswick)
506 643-7856
to-linh.huynh@fcnb.ca

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

Susan Pawelek
Accountant
Compliance and Registrant Regulation Branch
Commission des valeurs mobilières de l'Ontario
416 593-3680
spawelek@osc.gov.on.ca

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

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