OSLER

Les ACVM publient des pratiques en matière de cybersécurité et de médias sociaux à l'intention des sociétés inscrites

26 OCTOBRE 2017 8 MIN DE LECTURE

Expertises Connexes

- Cybersécurité et intervention en cas d'incident lié à la sécurité
- Gestion de placements
- Respect de la vie privée et gestion de l'information

Auteurs(trice): Adam Kardash, Blair Wiley, Lori Stein

Les courtiers inscrits, les conseillers et les gestionnaires de fonds de placement sont confrontés à de plus en plus de menaces raffinées visant la sécurité des données qu'ils détiennent, notamment les renseignements personnels dont ils ont la charge et le contrôle.

Les Autorités canadiennes des valeurs mobilières (ACVM) ont, par conséquent, identifié la cybersécurité comme l'une de leurs priorités dans le Plan d'affaires des ACVM 2016-2019, et elles continuent de se concentrer sur cet enjeu puisqu'elles ont publié des indications précises sur les pratiques en matière de cybersécurité et de médias sociaux.

L'Avis 33-321 du personnel des ACVM : Cybersécurité et médias sociaux (l'« Avis »), publié le 19 octobre 2017, indique que les politiques et procédures en matière de cybersécurité des sociétés inscrites devraient inclure des mesures préventives, de la formation pour tous les employés et un plan d'intervention en cas de cyberincident. Les ACVM précisent également que le secteur financier est une cible bien connue des cybercriminels et que, par conséquent, des mesures de protection doivent être mises en place par toutes les sociétés inscrites dans le cadre de leurs systèmes de contrôle et de conformité afin de gérer les risques liés à leur activité conformément aux pratiques commerciales prudentes.

Contexte

L'Avis 11-332 du personnel des ACVM : Cybersécurité, publié en septembre 2016, informait les sociétés inscrites que leurs politiques et procédures en matière de cybersécurité seraient examinées dans le cadre des examens de conformité. Il décrivait également les sondages menés et les groupes de discussions mis sur pied par des membres des ACVM afin de recueillir des données sur les pratiques en matière de cybersécurité et les programmes de formation des sociétés inscrites.

L'Avis résume les résultats du sondage mené à l'automne 2016 envoyé à plus de 1 000 sociétés inscrites, auquel 63 % d'entre elles ont répondu. Environ 51 % des répondants ont été touchés par un incident de cybersécurité, notamment d'hameçonnage, de logiciels malveillants et de tentatives frauduleuses de se faire passer pour un client par courriel pour transférer des fonds ou des valeurs mobilières.

Cybersécurité

L'Avis énonce les attentes des ACVM selon lesquelles chaque société inscrite devrait i) établir des politiques et des procédures en matière de cybersécurité qui encadrent l'utilisation des communications et des appareils électroniques, la sécurité de réseau et la vérification des

directives transmises électroniquement par les clients; ii) donner de la formation régulière à tous les employés, relativement notamment à la reconnaissance des risques, aux types de cybermenaces et à la façon de signaler les cyberincidents; iii) mener un processus annuel d'évaluation des risques; iv) se doter d'un plan d'intervention en cas de cyberincident; v) évaluer les pratiques de cybersécurité de fournisseurs de services ayant accès à leurs réseaux et à leurs données; vi) mettre en place des mesures de protection des données, dont l'utilisation de chiffrement et de mots de passe sur tous les ordinateurs et les appareils électroniques; et vii) souscrire une assurance qui couvre adéquatement les risques de cybersécurité.

À la lumière des résultats du sondage présentés dans l'Avis, la majorité des sociétés inscrites devront améliorer leurs pratiques de cybersécurité au chapitre de la protection des données et de l'assurance pour se conformer aux exigences du personnel des ACVM. Seuls 48 % des répondants ont affirmé utiliser le chiffrement pour protéger les données des appareils électroniques portables, des ordinateurs de bureau, des fichiers de données ou des communications par courriel et pièces jointes et près de 60 % des répondants ont déclaré n'avoir aucune assurance relative à la cybersécurité. Bien que les indications des ACVM n'exigent pas explicitement que les sociétés inscrites utilisent le chiffrement et souscrivent une assurance relative à la cybersécurité, celles qui n'adopteront pas ces pratiques devront se préparer à expliquer leurs solutions de rechange pour gérer les risques de cybersécurité ciblés par ces pratiques.

En outre, 34 % des répondants n'ont aucun plan d'intervention en cas de cyberincident et 25 % de ceux qui en ont un ne l'ont pas encore mis à l'essai. Le personnel des ACVM s'attend à ce que le plan d'intervention en cas de cyberincident nomme les personnes responsables, décrive les différents types de cyberattaques, y compris les procédures visant à atténuer les dommages, à éradiquer la menace et à récupérer les données, et qu'il soit testé au moins une fois par année. Il devrait être précisé dans les politiques et procédures des sociétés inscrites que les cyberincidents et les cybermenaces doivent être déclarés au conseil d'administration ou au corps dirigeant.

Médias sociaux

L'Avis indique que les médias sociaux peuvent servir à perpétrer des cyberattaques, notamment à envoyer des courriels d'hameçonnage ou des liens menant à des sites Web installant des logiciels malveillants. Par conséquent, bien que les politiques de médias sociaux traitent généralement des pratiques de commercialisation, comme l'indique l'Avis 31-325 du personnel des ACVM : Pratiques de commercialisation des gestionnaires de portefeuille, les sociétés inscrites doivent également tenir compte des enjeux de cybersécurité lorsqu'ils rédigent ces politiques et veillent à leur application.

Les résultats du sondage indiquent que 77 % des répondants se sont dotés de politiques et de procédures en matière de médias sociaux et que 94 % des répondants surveillent les activités sur les médias sociaux d'une manière ou d'une autre. L'Avis indique qu'on peut faire mieux en ce qui a trait à la formation des employés, à la tenue des dossiers et aux lignes directrices relatives au retrait des publications désuètes sur les médias sociaux.

Le personnel des ACVM insiste sur l'importance des procédures d'approbation et de surveillance compte tenu de la facilité avec laquelle du contenu peut être publié sur les plateformes de médias sociaux, de la difficulté de le retirer une fois affiché et de la nécessité de réagir rapidement aux enjeux lorsqu'ils surviennent. Les ACVM s'attendent à ce que les sociétés inscrites soient en mesure de revoir, de surveiller, de conserver et de retirer tout contenu sur les médias sociaux, notamment les communications non autorisées des employés sur les médias sociaux, pour les sociétés qui ne permettent pas l'utilisation des médias sociaux à des fins commerciales.

Directives en matière de cybersécurité à l'intention des émetteurs

En février 2017, le personnel de la British Columbia Securities Commission, de la Commission des valeurs mobilières de l'Ontario et de l'Autorité des marchés financiers du Québec ont publié l'Avis multilatéral 51-347 du personnel des ACVM : Information sur les risques et les incidents liés à la cybersécurité, qui énonce des indications à l'intention des émetteurs canadiens relatives aux pratiques de communication de l'information. Consultez notre bulletin Actualité Osler qui résume l'avis multilatéral.

Conclusion

Le personnel des ACVM précise que les indications en matière de cybersécurité s'appliquent à toute société, peu importe sa taille, son moment d'inscription, ou dans quelle mesure elle se fie aux mesures de protection instaurées par ses fournisseurs de services ou ses sociétés affiliées. L'Avis contient des liens vers des ressources offertes par l'Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM), l'Association canadienne des courtiers de fonds (ACFM) et le Bureau du surintendant des institutions financières (BSFI) afin d'aider les sociétés à évaluer leurs pratiques actuelles en matière de cybersécurité.

Comment Osler peut-il vous aider?

Osler conseille régulièrement des organisations de tous les secteurs (y compris des services financiers) sur la sécurité de l'information et la gouvernance des données, notamment en ce qui a trait au développement de protocoles de préparation et d'intervention en cas d'incidents. Nous avons agi dans les plus importants incidents relatifs à la sécurité à ce jour. Grâce à notre expertise de pointe reconnue mondialement tant en conformité réglementaire en matière de sécurité, qu'en protection de la vie privée et des données, notre équipe est en mesure de vous fournir des conseils pratiques et interdisciplinaires dans ce secteur complexe qui évolue rapidement.

Pour obtenir de plus amples renseignements, veuillez communiquer avec Lori Stein, Blair Wiley ou Adam Kardash.