

COMMUNIQUÉ

Pour diffusion immédiate

*Pour de plus amples renseignements, veuillez
communiquer avec la personne-ressource ci-dessous.*

Andrea Zviedris
Chef des relations avec les médias
et des affaires publiques
416 943-6906
azviedris@iroc.ca

Les sociétés de placement réglementées par l'OCRCVM améliorent leur état de préparation en matière de cybersécurité

Les résultats d'un sondage montrent des améliorations sur le plan de la formation, des plans d'intervention en cas d'incident et de l'évaluation des risques présentés par les tiers

Le 2 avril 2019 (Toronto, Ontario) – Selon un sondage mené auprès de toutes les sociétés réglementées par l'Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM), les sociétés de placement canadiennes ont pris des mesures concrètes pour mettre en place des programmes de cybersécurité visant à gérer les menaces et à protéger leurs clients et leurs activités.

Les sociétés ont répondu à ce sondage en novembre 2018, et nous avons évalué leurs réponses au regard d'un cadre de cybersécurité mis au point par le National Institute of Standards and Technology. Ce cadre est axé sur la gouvernance, le degré de sécurité, le degré de vigilance et la résilience des sociétés. Nous avons communiqué à chaque société les résultats de l'évaluation et leur avons indiqué les lacunes en matière de cybersécurité qui devraient être traitées en priorité. Ce sondage faisait suite à un premier sondage mené en 2016.

En voici les points saillants :

- Presque toutes les sociétés (94 %) évaluent les cyberrisques que présentent les tiers avant de conclure un contrat avec ceux-ci – en 2016, cette proportion était de 70 %;
- 82 % des sociétés donnent à leurs employés une formation sur la cybersécurité au moins une fois par année – comparativement à 56 % en 2016;
- 72 % des sociétés sont dotées d'un plan d'intervention en cas d'incident – par rapport à 53 % en 2016;
- Plus de la moitié (55 %) des sociétés a acheté une police de cyberassurance – comparativement à 37 % en 2016;
- De 2016 à 2018, le nombre de sociétés présentant un risque élevé de subir une cyberattaque a diminué – les petites sociétés ayant le plus contribué à cette baisse.

Les résultats du sondage permettent aux sociétés de cibler les domaines où elles peuvent augmenter encore plus leur degré de préparation en matière de cybersécurité, par exemple en effectuant des évaluations des répercussions ou du risque lié aux renseignements personnels, ou en surveillant le Web invisible pour détecter les renseignements les concernant qui y circulent.

« L'OCRCVM travaille étroitement avec les sociétés pour gérer les risques liés à la cybersécurité et protéger les données, dans le cadre de son mandat qui consiste à protéger les investisseurs et à maintenir l'intégrité des marchés, a déclaré Louis Piergeti, vice-président à la conformité des finances et des opérations de l'OCRCVM. L'augmentation marquée du nombre de sociétés qui ont apporté des changements importants à leur programme de cybersécurité montre qu'elles tiennent à protéger leurs clients des futures menaces. »

Le mois dernier, l'OCRCVM, en collaboration avec Accenture, a publié un rapport qui s'intitule « Favoriser l'évolution des services-conseils au Canada ». Ce rapport [est le résultat d'une vaste consultation en plusieurs phases qui a été menée](#) pour mieux comprendre la façon dont le secteur évolue dans le but de répondre aux besoins des investisseurs et comment la réglementation peut mieux favoriser l'innovation. Ainsi, l'OCRCVM s'engage à maintenir le dialogue avec les sociétés de placement à mesure qu'elles s'adaptent aux transformations du secteur et aux innovations technologiques, notamment au moyen de programmes de cybersécurité.

L'OCRCVM a aussi proposé une règle sur le [signalement obligatoire des incidents de cybersécurité](#), laquelle pourrait l'aider à déterminer si les sociétés ont besoin d'être conseillées sur la façon d'évaluer et de réduire toute responsabilité potentielle. L'OCRCVM sera aussi en mesure de juger si les renseignements recueillis pourraient servir à améliorer l'état de préparation de l'ensemble du secteur.

Également, en 2018, l'OCRCVM a organisé un événement d'une journée destiné aux sociétés de petite et de moyenne taille pendant lequel les participants ont pris part à des exercices de simulation de cyberincidents tels qu'une attaque par rançongiciel, une fuite de données ou une atteinte à la sécurité des renseignements de tiers. À la fin des exercices, des experts en cybersécurité, en réglementation et en droit ont donné des conseils et recommandé des solutions efficaces aux participants.

L'OCRCVM a aussi publié un [Guide de pratiques exemplaires en matière de cybersécurité](#) destiné aux sociétés et aux conseillers.

À propos de l'OCRCVM

L'OCRCVM est l'organisme d'autoréglementation national qui surveille l'ensemble des courtiers en placement et toutes les opérations que ceux-ci effectuent sur les marchés des titres de capitaux propres et des titres de créance au Canada. L'OCRCVM établit la réglementation en matière de commerce des valeurs mobilières, veille à la protection des investisseurs et renforce l'intégrité des marchés tout en favorisant des marchés financiers sains au Canada. Il s'acquitte de ses responsabilités de réglementation en établissant et en faisant appliquer des règles qui régissent la compétence, les activités et la conduite financière de plus de 170 courtiers en placement canadiens et des quelque 29 000 employés inscrits qui y travaillent, dont la plupart sont communément appelés conseillers en placement. L'OCRCVM établit et fait appliquer également des règles d'intégrité du marché qui régissent les opérations effectuées sur les marchés canadiens des titres de capitaux propres et des titres de créance.