

AVIS DE L'OCRCVM

Avis sur les règles

Avis technique

Règles des courtiers membres

Destinataires à l'interne :

Affaires juridiques et conformité

Haute direction

Opérations

Personne-ressource :

Louis Piergeti

Vice-président à la conformité des finances et des opérations

416 646-3026

lpiergeti@iiroc.ca

18-0063

Le 22 mars 2018

Signalement des incidents de cybersécurité

Les cyberattaques sont de plus en plus nombreuses et sophistiquées. On constate en particulier une augmentation générale des attaques perpétrées par rançongiciel. Ce phénomène est probablement attribuable à la « banalisation » des outils, qui peuvent maintenant être utilisés par des assaillants moins expérimentés. La gestion active des cyberrisques est essentielle à la stabilité des courtiers membres de l'OCRCVM (**courtiers**), à l'intégrité des marchés financiers et à la protection des investisseurs. Au cours des dernières années, nous nous sommes engagés à aider les courtiers à renforcer leurs méthodes de gestion des risques et à accroître leur capacité d'intervention en matière de cybersécurité.

Afin de mieux outiller les courtiers et de les aider à gérer ces risques, nous publierons bientôt un appel à commentaires au sujet d'un projet de modification des Règles des courtiers membres, qui prévoit le signalement obligatoire de certains incidents de cybersécurité.

En attendant, nous demandons à tous les courtiers de nous signaler promptement tout incident de cybersécurité qui est survenu au sein de leur société.

Le [Guide de pratiques exemplaires en matière de cybersécurité](#) et le [Guide de planification – Gestion des cyberincidents](#) établissent des normes sectorielles et des pratiques exemplaires pour aider les



courtiers à gérer les cyberrisques. Un élément important traité dans ces documents est l'échange rapide de renseignements dans le but d'atténuer les cyberrisques. Grâce à un signalement rapide des incidents à l'OCRCVM, nous pouvons :

- aider immédiatement le courtier à réagir à un incident de cybersécurité;
- alerter d'autres courtiers à propos des dangers et leur communiquer les pratiques exemplaires en matière d'interventions;
- évaluer les tendances et établir des données complètes sur la cybersécurité;
- promouvoir la confiance dans les courtiers et l'intégrité du marché.

Pour signaler un incident de cybersécurité, veuillez communiquer avec le chef du Service de la conformité des finances et des opérations de l'OCRCVM responsable de votre société.