OSLER

Avis multilatéral 51-347 du personnel des ACVM – Information sur les risques et les incidents liés à la cybersécurité

9 FÉVRIER 2017 7 MIN DE LECTURE

Expertises Connexes

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

Auteurs(trice): Robert Anton, Blair Wiley, Daniel Kolibar

Contexte

Dans le cadre des efforts soutenus que déploient les Autorités canadiennes en valeurs mobilières (ACVM) pour mettre en lumière les risques liés à la cybersécurité auxquels sont exposés les émetteurs, les personnes inscrites et autres entités réglementées, le personnel de la British Columbia Securities Commission, de la Commission des valeurs mobilières de l'Ontario et de l'Autorité des marchés financiers (personnel) a récemment publié l'Avis multilatéral 51-347 du personnel des ACVM, *Information sur les risques et les incidents liés à la cybersécurité* [PDF] (l'avis du personnel).

L'avis du personnel, destiné aux émetteurs canadiens, découle d'un récent examen de l'information fournie sur la cybersécurité. Le personnel a passé en revue les derniers dépôts de 240 entreprises constituant l'indice composé S&P/TSX pour évaluer l'information fournie sur les facteurs de risque liés à la cybersécurité et sur les cyberincidents. L'examen avait une portée plus étendue que les examens passés et témoigne de l'opinion du personnel selon laquelle les émetteurs dans tous les secteurs peuvent être exposés aux risques liés à la cybersécurité.

Information sur les facteurs de risque

L'examen du personnel concernant l'information sur les facteurs de risque a révélé que 61 % des émetteurs soumis à l'examen traitaient des questions de cybersécurité dans leur information sur les facteurs de risque et que 20 % des émetteurs soumis à l'examen indiquaient avoir confié à une personne, à un groupe ou à un comité la responsabilité de leur stratégie en matière de cybersécurité, le plus souvent au comité d'audit. L'examen du personnel a permis de constater que les émetteurs mettaient généralement l'accent sur leur dépendance envers les technologies de l'information, bien que certains d'entre eux aient mentionné des facteurs propres à eux comme le secteur, les actifs précis dont ils étaient propriétaires, la nature de leurs activités ou leur qualité d'entrepreneurs du gouvernement comme des facteurs augmentant les risques liés à la cybersécurité.

L'information sur les risques liés à la cybersécurité devrait figurer dans les documents déposés par un émetteur si le risque est important pour lui. Le personnel recommande de déterminer l'importance des risques liés à la cybersécurité par une évaluation de la probabilité qu'une atteinte se produise et l'ampleur prévue de son incidence. Le personnel a aussi reconnu que tous les émetteurs dépendent de plus en plus des technologies de l'information et qu'ils sont tous exposés à une cyberattaque, suggérant ainsi que les ACVM s'attendent à ce que les émetteurs soient plus nombreux à fournir de l'information sur les

risques liés à la cybersécurité.

Le personnel s'attend à ce que l'information sur les facteurs de risque porte surtout sur les risques importants propres à l'émetteur et à sa situation, sans formules toutes faites ou générales. Les émetteurs ont donc le fardeau de rédiger une information sur les facteurs de risque qui tient compte des éléments suivants : (i) les formes et les sources de l'exposition à la cybersécurité, (ii) le niveau d'exposition et les motifs qui le sous-tendent, (iii) la capacité de réaction de l'émetteur au risque, (iv) les conséquences possibles d'une cyberattaque et (v) les incidents importants antérieurs, ou la série d'incidents, liés à la cybersécurité et leurs effets sur les risques liés à la cybersécurité de l'émetteur – tous ces éléments sont conformes aux indications concernant l'information sur la cybersécurité publiées par la Securities and Exchange Commission (SEC) des États-Unis et les indications préparées par l'Organisation internationale des commissions de valeurs (OICV) dans son rapport sur la cybersécurité dans les marchés des valeurs mobilières [PDF].

Le personnel s'attend également à ce que les émetteurs présentent la façon dont ils réduisent les risques liés à la cybersécurité et leur dépendance envers des tiers experts en ce qui a trait à la stratégie ou aux mesures correctives en matière de cybersécurité. Les indications de la SEC et de l'OICV comportent des suggestions similaires. Par contre, les émetteurs doivent se rappeler que les exigences de forme concernant l'information sur les facteurs de risque leur imposent de ne pas minimiser un facteur de risque en l'assortissant de réserves ou de conditions excessives. Ils doivent donc décrire les efforts qu'ils ont consacrés à la réduction des cyberattaques sans diminuer l'information sur les facteurs de risque liés à la cybersécurité ni y mettre de bémol.

Information sur les cyberincidents

L'avis du personnel traite aussi de l'information sur les cyberincidents. Si l'information sur les facteurs de risque liés à la cybersécurité est relativement courante dans les documents déposés auprès des autorités en valeur mobilières, le personnel a par contre constaté que les émetteurs déclarent rarement les cyberincidents. Dans les documents récemment examinés par le personnel, aucun émetteur n'avait rapporté de cyberincident important.

L'avis du personnel rappelle aux émetteurs qu'ils doivent déclarer un cyberincident (ou des cyberincidents) conformément à la législation en valeurs mobilières s'il constitue un fait ou un changement important pour l'entreprise de l'émetteur. Le personnel signale ce qui suit concernant l'évaluation de l'importance d'un cyberincident :

- Il n'existe aucun critère de démarcation, et le seuil que doit franchir un cyberincident pour devenir important variera d'un émetteur et d'un secteur à l'autre.
- Il faut analyser le contexte du cyberincident. Le personnel mentionne qu'un cyberincident isolé peut ne pas être important, mais qu'une série d'incidents mineurs peut devenir importante selon le type de perturbation causée.
- Les cyberincidents peuvent ne pas être détectés immédiatement et il peut être difficile d'évaluer leur gravité. C'est pourquoi le personnel rappelle que pour déterminer l'importance d'un cyberincident il faut nécessairement lancer un processus dynamique comportant les phases de détection, d'évaluation et de prise de mesures correctives.

Les ACVM s'attendent à ce que l'émetteur qui a adopté un plan de reprise en matière de cybersécurité y mentionne comment il évaluera l'importance d'un cyberincident afin de déterminer s'il le déclarera et, dans l'affirmative, comment il le déclarera. Si un émetteur juge qu'un cyberincident doit être déclaré, le personnel recommande que l'émetteur envisage d'en communiquer les répercussions et les coûts prévus. Dans un même ordre d'idées, le

personnel s'attend à ce que les émetteurs tenus d'établir et de maintenir des contrôles et des procédures de communication de l'information appliquent ces contrôles et ces procédures aux cyberincidents détectés, veillant ainsi à ce que ces incidents soient bien communiqués à la direction et que la décision de les déclarer soit prise rapidement.

* * * *

Veuillez communiquer avec les auteurs si vous avez des questions concernant l'avis du personnel ou avez besoin d'aide concernant l'information sur les facteurs de risque liés à la cybersécurité, l'information sur les cyberincidents ou les plans de reprise en matière de cybersécurité.