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

Avis 11-332 du personnel des ACVM
Cybersécurité

Le 27 septembre 2016

Introduction

Le 26 septembre 2013, les Autorités canadiennes en valeurs mobilières (les « ACVM ») ont publié l'Avis 11-326 du personnel des ACVM, *Cybersécurité* (l'« avis de 2013 »), qui précisait que les contrôles implantés par les émetteurs, les personnes inscrites et les entités réglementées (collectivement, les « participants au marché ») passent impérativement par des mesures rigoureuses et personnalisées en matière de cybersécurité[1]. Les participants au marché étaient invités à adopter des mesures de protection adéquates pour se protéger, ainsi que leurs clients ou les parties intéressées. Les mesures décrites dans l'avis de 2013 sont notamment les suivantes :

- sensibiliser le personnel à l'importance de la cybersécurité et au rôle qu'il a à jouer à cet égard;
- suivre les indications et les meilleures pratiques des associations professionnelles et des organismes reconnus en sécurité informatique;
- s'il y a lieu, procéder régulièrement à des tests et à des évaluations de la vulnérabilité et de la sécurité chez les tiers;
- revoir régulièrement les mesures de contrôle du risque lié à la cybersécurité.

Depuis la publication de l'avis de 2013, le contexte de la cybersécurité a considérablement évolué, les cyberattaques devenant plus fréquentes, complexes et coûteuses pour les organisations. Les ACVM publient donc le présent avis pour :

- insister de nouveau sur l'importance des cyberrisques pour les participants au marché;
- informer les parties intéressées sur les projets récents et à venir des ACVM;
- indiquer les normes existantes et les travaux publiés, notamment ceux de l'Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM), de l'Association canadienne des courtiers de fonds mutuels (ACFM) et des organismes internationaux de réglementation et de normalisation;
- communiquer les attentes générales à l'égard des cadres de cybersécurité des participants au marché;
- examiner les façons de coordonner la communication et l'échange d'information entre organismes de réglementation et participants au marché.

[1] Au nombre des entités réglementées, on compte les organismes d'autoréglementation, les marchés, les chambres de compensation et les agences de traitement de l'information.

Évolution du contexte des cybermenaces

Le contexte des cybermenaces évolue au rythme des percées technologiques et de l'émergence de nouvelles stratégies commerciales. Compte tenu des liens électroniques entre les acteurs du système financier, une cyberattaque peut avoir rapidement des répercussions l'importantes, nuire à l'intégrité et à l'efficience des marchés mondiaux et ébranler la confiance dans le système.

Dans un contexte d'évolution technologique, les cyberadversaires disposent de moyens de plus en plus perfectionnés et sont en mesure de causer des dommages de plus en plus graves. Le nombre d'entités victimes de pertes financières, de vol de propriété intellectuelle, d'atteinte à la réputation et de fraude ou visées par des poursuites est en hausse.

Certaines études portant sur l'incidence des atteintes à la cybersécurité, comme celles publiées par le Ponemon Institute[2] et PricewaterhouseCoopers[3], formulent les conclusions suivantes :

- en 2015, le nombre d'incidents détectés a augmenté de 38 % par rapport à 2014;
- le coût total moyen d'une atteinte à la protection des données s'établissait à 4 millions de dollars américains chez les sociétés ayant participé au sondage 2016 de Ponemon.

Compte tenu de ces tendances ainsi que des récents cas de piratage hautement médiatisés, les autorités internationales étudient ou mettent en œuvre diverses mesures afin d'inciter les participants au marché à améliorer leurs cyberdéfenses.

Cybersécurité : une priorité pour les ACVM

Les ACVM ont fait de la cybersécurité une priorité de leur plan d'affaires 2016-2019, et certains de leurs membres ont également adopté cette orientation. C'est pourquoi elles font un travail de sensibilisation et de promotion de la résilience à cet égard. Elles s'attachent surtout à :

- améliorer la collaboration et la communication avec les participants au marché sur les enjeux de cybersécurité;
- évaluer le niveau de résilience des participants au marché en matière de cybersécurité, notamment les mesures de protection des données personnelles des investisseurs;
- améliorer la compréhension, chez les participants au marché, des activités de surveillance de la cybersécurité menées par les membres des ACVM, et notamment leur indiquer les attentes concernant leur préparation en matière de cybersécurité[4].

Puisque le secteur des services financiers est une cible de choix pour les cyberattaques, les ACVM jouent un rôle central dans l'évaluation et la promotion de la préparation et de la cyberrésilience auprès des participants au marché.

---

[2] *2016 Cost of Data Breach Study: Global Analysis*. Cette analyse comparative parrainée par IBM et menée de façon indépendante par le Ponemon Institute LLC porte sur 383 sociétés réparties dans 12 pays.

[3] *The Global State of Information Security Survey 2016* est une étude effectuée annuellement à l'échelle mondiale par PwC, CIO et CSO qui analyse les réponses de plus de 10 000 chefs de la direction, chefs des finances, chefs de l'information, chefs de la sécurité des systèmes d'information, chefs de la sécurité, vice-présidents et directeurs des technologies de l'information ainsi que les pratiques en matière de sécurité de 127 pays.

[4] Source : http://www.autorites-valeurs-mobilieres.ca/presentation_des_ACVM.aspx?ID=1504&LangType=1036.

Projets récents et à venir des ACVM

Depuis la publication de l'avis de 2013, les ACVM surveillent l'évolution de la situation et ont entrepris un certain nombre de projets visant à intégrer la cybersécurité dans leurs travaux et à échanger avec le secteur et les parties intéressées. L'objectif poursuivi est de mieux comprendre l'environnement, les défis et le degré de préparation des participants au marché et d'améliorer globalement la résilience dans nos marchés. Voici un survol des projets récents et à venir des ACVM.

Émetteurs : l'avis de 2013 indiquait que les émetteurs devraient évaluer si les cyberrisques auxquels ils sont exposés, les contrôles qu'ils ont mis en place pour les gérer et les incidents qui pourraient survenir à cet égard sont des éléments qui devraient être communiqués dans un prospectus ou tout autre document d'information continue. Depuis lors, certains membres des ACVM ont examiné l'information communiquée par les émetteurs pour en analyser le contenu sous l'angle des risques liés à la cybersécurité et des cyberattaques. Les examens étaient généralement axés sur les facteurs de risque, les poursuites et la gouvernance. Bon nombre d'émetteurs n'avaient aucune information ou n'avaient que de l'information passe-partout ne portant sur aucune entité en particulier.

Les membres des ACVM comptent revoir l'information fournie par certains grands émetteurs dans les mois à venir et communiquer avec eux, le cas échéant, pour comprendre leur évaluation de l'importance des risques liés à la cybersécurité et des cyberattaques. Les conclusions et recommandations découlant de ces examens seront publiées ultérieurement.

Personnes inscrites : dans le cadre des examens de conformité, le personnel des ACVM échange en permanence avec les sociétés inscrites au sujet des politiques et procédures de cybersécurité, notamment en ce qui concerne :

- les programmes des sociétés en matière d'évaluation des risques liés à la cybersécurité et de gouvernance de la sécurité de l'information;
- les mesures de protection et de contrôle prises par les sociétés en matière de technologies de l'information;
- l'utilisation du chiffrement;
- les risques liés aux fournisseurs de services;
- les essais de vulnérabilité et la surveillance de la conformité;
- les preuves que la formation et la sensibilisation des employés sont assurées régulièrement;
- les plans d'intervention en cas d'incidents;
- les pratiques en matière d'acceptation des instructions données par les clients pour retirer et transférer des fonds de façon électronique.

Certains membres des ACVM recueillent actuellement des données sur les pratiques des personnes inscrites en matière de cybersécurité. En mai 2016, un questionnaire sur l'évaluation des risques a été envoyé à un nombre important de sociétés inscrites afin de recueillir des données fondamentales sur leurs pratiques en la matière et leurs programmes de formation. Un autre membre a mis sur pied simultanément un groupe de discussion composé de personnes inscrites afin d'échanger sur leurs préoccupations, d'examiner les façons de les sensibiliser

davantage et de leur offrir du soutien en gestion des risques liés à la cybersécurité. Un examen sur dossier plus ciblé est prévu pour le reste de 2016 afin d'approfondir les points abordés dans les examens de conformité courants.

Entités réglementées : l'examen indépendant des systèmes que les marchés, chambres de compensation et agences de traitement de l'information doivent effectuer a toujours eu une composante cybersécurité. Or, depuis 2013, il porte expressément sur cet enjeu pour l'ensemble des entités réglementées. Par ailleurs, les référentiels centraux qui exercent des activités au Canada depuis l'automne 2014 ont des obligations semblables. De plus, les ACVM ont recueilli des renseignements afin de mieux comprendre où les entités réglementées en sont pour ce qui est de l'adoption de cadres de cybersécurité adéquats afin de mieux gérer et de réduire les cyberrisques[5].

Un membre des ACVM s'est aussi penché sur les interconnexions, les principales interdépendances de traitement et les points de défaillance pour mieux comprendre l'incidence et la contagion potentielles en cas d'attaque contre une entité réglementée ou un site.

Activités internationales : le personnel des ACVM a participé aux travaux de l'OICV, notamment avec le CPIM, sur le cyberrisque et la cyberrésilience. Il s'agissait notamment d'élaborer des cadres de cyberrésilience et de publier des rapports sur des approches et des outils réglementaires conçus pour régler les questions de cybersécurité et sur des mécanismes permettant aux places de négociation de gérer efficacement les risques qui y sont liés.

Les projets actuels portent sur l'amélioration de l'échange d'information sur la cybersécurité entre organismes de réglementation internationaux et s'appuient sur l'Accord multilatéral de l'OICV aux fins d'enquête sur les manipulations du marché et infractions liées à la cybersécurité.

Ressources existantes en matière de cybersécurité

Divers organismes de réglementation et de normalisation ont publié de l'information et des directives pour favoriser l'échange de renseignements sur les cybermenaces, améliorer la préparation aux cyberincidents ainsi qu'informer et sensibiliser les parties intéressées aux enjeux et risques liés à la cybersécurité. Voici plusieurs documents de référence qui pourraient être utiles aux participants au marché :

Indications du CPIM et l'OICV sur la cyberrésilience pour les infrastructures du marché financier
http://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf

Projets du Federal Financial Institutions Examination Council (FFIEC) en matière de cybersécurité
http://www.ffiec.gov/cybersecurity.htm

[5] Un cadre de cybersécurité consiste en un ensemble de ressources organisationnelles, notamment des politiques, du personnel, des processus, des pratiques et des technologies servant à évaluer et à atténuer les cyberrisques et les cyberattaques.

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

Rapport de l'OICV sur la cybersécurité dans les marchés des valeurs mobilières
http://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf

Rapport de l'OICV sur les mécanismes permettant aux places de négociation de gérer efficacement les risques liés aux opérations électroniques et les plans de continuité des activités
http://www.iosco.org/library/pubdocs/pdf/IOSCOPD522.pdf

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

Document de la Securities Industry and Financial Markets Association (SIFMA) intitulé *Principles for Effective Cybersecurity Regulatory Guidance*
http://www.sifma.org/issues/item.aspx?id=8589951691

Document de la SIFMA intitulé *Guidance for Small Firms: How Small Firms Can Protect Their Business*
http://www.sifma.org/issues/operations-and-technology/cybersecurity/guidance-for-small-firms/

Document de la Financial Industry Regulatory Authority (FINRA) intitulé *Report on Cybersecurity Practices*
https://www.finra.org/file/report-cybersecurity-practices

Cadre de cybersécurité du National Institute for Standards and Technology (NIST)
http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.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

Directives sur l'information à fournir de la Division of Corporation Finance de la Securities and Exchange Commission (SEC)
https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Ces ressources tendent à démontrer qu'il n'existe pas qu'une seule façon d'assurer la cybersécurité et que les organismes doivent établir leur cadre en conséquence. Les publications susmentionnées soulignent notamment la nécessité pour les organismes de faire ce qui suit :

- gérer la cybersécurité au niveau organisationnel et attribuer à la direction et au conseil la responsabilité de la gouvernance avec obligation de rendre des comptes;
- encadrer leurs activités de cybersécurité selon ces principes : préciser, protéger, détecter, intervenir et reprendre;

- établir et maintenir un programme rigoureux de sensibilisation à la cybersécurité à l'intention de leur personnel;
- formuler une compréhension claire des facteurs opérationnels et des enjeux de sécurité propres à leur utilisation de la technologie, des systèmes et des réseaux;
- comprendre la probabilité qu'un événement survienne ainsi que son incidence afin de déterminer le degré de risque acceptable selon leur tolérance au risque et leurs obligations budgétaires et juridiques;
- gérer l'exposition aux cyberrisques découlant du recours à des fournisseurs de services;
- envisager des méthodes de protection des renseignements personnels et tenir compte de toute obligation de déclarer les atteintes à la cybersécurité à un organisme de réglementation;
- envisager d'échanger de l'information sur les cyberincidents avec les participants au marché;
- communiquer, collaborer et coordonner les efforts avec d'autres entités;
- établir en temps opportun des plans de rétablissement des capacités ou des services touchés par un cyberincident;
- traiter les programmes de cybersécurité comme des projets dynamiques et évolutifs devant être actualisés et améliorés de façon continue.

Prochaines étapes et attentes des ACVM

Bien que les participants au marché prennent déjà des mesures pour comprendre et atténuer les risques liés à la cybersécurité, il importe de faire preuve de vigilance en tout temps. Les ACVM comptent tenir des tables rondes au cours des prochains mois pour échanger sur les enjeux et les risques, leurs attentes et le besoin de coordination. De plus amples renseignements seront communiqués ultérieurement, mais les objectifs généraux des tables rondes seront les suivants :

- promouvoir un dialogue ouvert avec les experts en cybersécurité et les participants au marché;
- faire le point sur la situation en matière de cyberrisques et les façons de les gérer;
- trouver des occasions d'améliorer la collaboration et la communication sur les enjeux communs de cybersécurité;
- échanger sur la coordination en cas de cyberincident.

Dans l'intervalle, nous nous attendons à ce que les participants au marché prennent les mesures nécessaires pour se protéger contre les cybermenaces. En particulier :

- *Émetteurs* : de façon générale, si un émetteur a déterminé que le cyberrisque est important, les membres des ACVM s'attendent à ce qu'il fournisse de l'information aussi détaillée que possible sur les risques qu'il court dans sa situation. Par ailleurs, les émetteurs devraient préciser dans tout plan de reprise après une cyberattaque la façon dont l'importance d'une attaque serait évaluée pour établir si de l'information doit être rendue publique à son sujet, à quel moment et de quelle façon. Dans le cadre de l'évaluation, les émetteurs devraient tenir compte de l'incidence sur leurs activités, leur réputation, leurs clients, leurs employés et leurs investisseurs.
- *Personnes inscrites* : les membres des ACVM s'attendent à ce que les personnes inscrites maintiennent leur vigilance lors de l'établissement, de la mise en œuvre et de l'actualisation de leurs mesures de protection et de gestion en matière de cybersécurité. Elles devraient

également consulter et suivre les directives publiées par des organismes d'autoréglementation comme l'OCRCVM et l'ACFM.

- *Entités réglementées* : les membres des ACVM s'attendent à ce que les entités réglementées vérifient leur conformité aux obligations continues prévues par la législation en valeurs mobilières et les modalités des décisions de reconnaissance, de leur inscription ou des dispenses, ce qui nécessite notamment de se doter de contrôles internes des systèmes et de déclarer les atteintes à la sécurité. Nous nous attendons également à ce que ces entités adoptent un cadre de cybersécurité établi par un organisme de réglementation ou de normalisation qui convienne à leur taille et à leur importance.

Renseignements :

Philippe Bergevin
Économiste principal
Affaires internationales et vigie stratégique
Autorité des marchés financiers
514 395-0337, poste 4285
philippe.bergevin@lautorite.qc.ca

Jean Lorrain
Directeur principal des affaires internationales et de la vigie stratégique
Autorité des marchés financiers
514 395-0337, poste 4311
jean.lorrain@lautorite.qc.ca

Tom Graham
Director, Corporate Finance
Alberta Securities Commission
403 297-5355
tom.graham@asc.ca

Isaac Z. Filaté
Senior Legal Counsel, Capital Markets Regulation Division
British Columbia Securities Commission
604 899-6573
ifilate@bcsc.bc.ca

Chris Besko
Directeur par intérim
Commission des valeurs mobilières du Manitoba
204 945-2561
cbesko@gov.mb.ca

Jeff Mason
Surintendant des valeurs mobilières
Ministère de la justice
Gouvernement du Nunavut
867 975-6591
jmason@gov.nu.ca

Jake van der Laan
Directeur, Application de la loi et Directeur de l'informatique
Commission des services financiers et des services aux consommateurs
Nouveau-Brunswick
506 658-6637
jake.vanderlaan@fcnb.ca

Tracey Stern
Manager, Market Regulation
Commission des valeurs mobilières de l'Ontario
416 593-8167
tstern@osc.gov.on.ca

John O'Brien
Superintendent of Securities
Office of the Superintendent of Securities
Terre-Neuve-et-Labrador
709 729-4909
johnobrien@gov.nl.ca

Alex Petro
Trading Specialist, Market Regulation
Commission des valeurs mobilières de l'Ontario
416 263-3796
apetro@osc.gov.on.ca

Tom Hall
Surintendant des valeurs mobilières
Bureau du surintendant des valeurs mobilières
Territoires du Nord-Ouest
867 767-9305
tom_hall@gov.nt.ca

Steven Dowling
Acting Director
Gouvernement de l'Île-du-Prince-Édouard
Superintendent of Securities
902 368-4551
sddowling@gov.pe.ca

Jack Jiang
Securities Analyst, Corporate Finance
Nova Scotia Securities Commission
902 424-7059
jack.jiang@novascotia.ca

Dean Murrison
Director, Securities Division
Financial and Consumer Affairs Authority of Saskatchewan
306 787-5879
dean.murrison@gov.sk.ca

Rhonda Horte
Securities Officer
Bureau du surintendant des valeurs mobilières
867 633-7969
rhonda.horte@gov.yk.ca