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

Avis 11-336 du personnel des ACVM
Résumé de la table ronde des ACVM sur les mesures à prendre en cas de cyberincident

Le 6 avril 2017

Le 27 février 2017, les Autorités canadiennes en valeurs mobilières (ACVM) ont tenu une table ronde pour débattre des questions de cybersécurité et des possibilités d'améliorer la collaboration, la communication et la coordination en cas de cyberincident de grande envergure. Le présent avis du personnel donne un aperçu des thèmes abordés et des principaux points à retenir.

Les participants à la table ronde représentaient un large éventail d'intervenants du marché canadien des valeurs mobilières (notamment des marchés, des chambres de compensation, des personnes inscrites, des émetteurs assujettis, des organismes de réglementation et des experts en cybersécurité) et une diversité de rôles et de points de vue. L'annexe du présent avis contient la liste des organisations participantes.

La table ronde a pris la forme de discussions autour de deux scénarios de cyberincident hypothétiques qui visaient, d'une part, à analyser la manière dont les participants réagiraient, individuellement et en tant que groupe, en cas d'incident de grande envergure et, d'autre part, à mieux comprendre les rôles joués par les entités et les organismes de réglementation pour ce qui est de la réaction à un incident, de la coordination et du partage d'information.

Dans le premier scénario, des chambres de compensation avaient été victimes d'un cyberincident à la suite duquel leurs systèmes de gestion du risque avaient généré des exigences de marge inexactes pour leurs membres. Dans le second, certains ordres transmis à un marché avaient été altérés, de sorte que des courtiers avaient obtenu de l'information erronée sur l'exécution des opérations.

Les discussions ont mis en évidence l'interdépendance des marchés des valeurs mobilières dans l'écosystème canadien ainsi que l'importance que revêtent la coopération et le partage d'information pour réagir à un cyberincident et réduire le risque de contagion. Selon les participants à la table ronde, les cyberincidents peuvent avoir de lourdes conséquences sur d'autres organisations que celles qui sont immédiatement concernées, surtout si les systèmes de base sont touchés.

De manière générale, les participants ont débattu des points suivants :

- la réaction des entités victimes d'un cyberincident, y compris les questions liées à la gouvernance, à l'évaluation des dommages, au personnel participant à la prise de décision et au flux d'information;

- la réaction des entités en aval et en amont de l'entité touchée, y compris les mesures à prendre pour réduire le plus possible les répercussions sur leur organisation;

- les personnes qui devraient participer aux discussions et à la prise de décision pour coordonner la réaction à un incident touchant l'ensemble du marché, notamment les organisations devant intervenir, les personnes responsables du processus de résolution ainsi que les modes de communication et de coordination entre les organisations;

- l'information devant être communiquée à l'interne et à l'externe, y compris les protocoles de communication des organisations et l'information que celles qui ne sont pas directement attaquées s'attendent à obtenir de l'entité visée;

- les facteurs susceptibles de contribuer à la coordination, à la communication et à la collaboration, y compris l'information nécessaire pour faciliter la coordination et la communication entre les intervenants, et les difficultés que les organisations peuvent avoir à surmonter pour y parvenir.

En particulier, les participants se sont penchés sur les éléments d'un solide plan d'intervention en cas d'incident (PII) pour les entités, y compris celles qui peuvent être indirectement touchées. Ils ont indiqué que les PII sont généralement très détaillés et exhaustifs en ce qui a trait aux procédures internes en cas d'incident, mais qu'ils devraient également traiter de la coordination et du partage d'information avec les autres intervenants, surtout en cas de cyberincident susceptible d'impliquer l'ensemble du marché.

Pour ce qui est du partage d'information et de la coopération entre les intervenants, les participants ont jugé généralement efficace de s'en remettre aux organisations existantes qui fournissent des services d'analyse et d'échange de renseignements, de même qu'aux réseaux de communication pair-à-pair informels. Néanmoins, des canaux de communication et une coordination plus structurés pourraient améliorer la capacité d'intervention et de reprise en cas de cyberincident à l'échelle du marché.

Les participants ont également discuté de la nécessité de tester et d'actualiser les PII, y compris les protocoles de coordination et de communication. Il est essentiel de faire régulièrement des exercices et des évaluations pour que les PII soient à jour et efficaces.

Enfin, il a été question des ressources privées et publiques vers lesquelles peuvent se tourner les organisations victimes d'un cyberincident : le Centre canadien de réponse aux incidents cybernétiques (CCRIC) de Sécurité publique Canada, la GRC, les corps policiers provinciaux et les organismes d'échange d'information comme le Financial Services Information Sharing and Analysis Center.

Tel qu'il est souligné dans l'Avis 11-332 du personnel des ACVM, *Cybersécurité*, 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. Ils s'attendent aussi 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.

Les ACVM ont fait de la cybersécurité une priorité de leur plan d'affaires 2016-2019. Par conséquent, à la lumière de la table ronde, leurs membres continueront de collaborer avec les participants au marché, les autres organismes de réglementation et les intervenants pour renforcer la préparation à d'éventuels cyberincidents, et élaboreront un processus de coordination plus structuré que ceux qui existent déjà.

Renseignements :

Philippe Bergevin
Économiste principal
Affaires internationales et vigie
Autorité des marchés financiers
philippe.bergevin@lautorite.qc.ca

Jean Lorrain
Directeur principal des affaires internationales et de la vigie stratégique
Autorité des marchés financiers
jean.lorrain@lautorite.qc.ca

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

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

Tom Graham
Director, Corporate Finance
Alberta Securities Commission
tom.graham@asc.ca

Jeff Mason
Surintendant des valeurs mobilières
Ministère de la Justice
Gouvernement du Nunavut
jmason@gov.nu.ca

Sasha Cekerevac
Regulatory Analyst, Equity Markets
Alberta Securities Commission
Sasha.Cekerevac@asc.ca

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

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

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

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

Steven Dowling
Acting Director
Gouvernement de l'Île-du-Prince-Édouard
Superintendent of Securities
sddowling@gov.pe.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
jake.vanderlaan@fcnb.ca

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

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

Rhonda Horte
Securities Officer
Bureau du surintendant des valeurs mobilières du Yukon
rhonda.horte@gov.yk.ca

Annexe – Liste des organisations participantes		
Neo Bourse Aequitas Inc.	eSentire Inc.	Banque Nationale du Canada
Bank of America	Fidessa group plc	NPC Dataguard
Banque du Canada	Financial Services Information Sharing and Analysis Center	Omega ATS
BMO Groupe financier	FundSERV Inc.	Bureau du surintendant des institutions financières (Canada)
Broadridge Financial Solutions	Greystone Managed Investments Inc.	Payments Canada
Office d'investissement du Régime de pensions du canada	Hedge Fund Standards Board	Sécurité publique Canada
Bourse des valeurs canadiennes	Société financière IGM Inc.	PwC Canada
CanDeal	Association canadienne du commerce des valeurs mobilières	RBC Marchés de capitaux
Banque CIBC	Organisme canadien de réglementation du commerce des valeurs mobilières	GRC
Deloitte S.E.N.C.R.L.	Investment Technology Group, Inc.	Ridge Canada
Ministère des Finances du Canada	KPMG Canada	Financière Sun Life
Groupe Desjardins	Lumen Asset Management Inc.	Groupe Financier Banque TD
Emera Inc	Association canadienne des courtiers de fonds mutuels	Groupe TMX Limitée
Ernst & Young s.r.l./S.E.N.C.R.L.	Nasdaq CXC Limited	