THE INVESTMENT FUNDS INSTITUTE OF CANADA

L'INSTITUT DES FONDS D'INVESTISSEMENT DU CANADA

GUIDE SUR LA CYBERSÉCURITÉ

octobre 2019

TABLE DES MATIÈRES

INTRODUCTION

Le Guide de pratiques exemplaires en matière de cybersécurité à l'intention des courtiers membres de l'OCRCVM mentionne que la cybersécurité a été définie de différentes façons par différents organismes.

> Le Comité sur les systèmes nationaux de sécurité (CNSS-4009) définit la cybersécurité comme la capacité d'une entreprise de protéger ou de défendre l'utilisation du cyberespace contre une attaque dans le cyberespace ayant pour but de désorganiser, de désactiver, de détruire ou de contrôler de façon malveillante un milieu ou une infrastructure informatique; ou de détruire l'intégrité des données ou de voler des renseignements contrôlés.
>
> Le National Institute of Standards and Technology définit ainsi la cybersécurité : « processus qui consiste à protéger l'information en empêchant les attaques et en intervenant en conséquence ». À l'instar du risque financier et du risque d'atteinte à la réputation, le risque de cybersécurité affecte le résultat d'une société. Il peut majorer les coûts et influer sur les revenus. Il peut porter atteinte à la capacité d'une organisation d'innover, de recruter et de conserver des clients.
>
> L'Organisation internationale de normalisation définit la cybersécurité ou la sécurité du cyberespace comme la préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information dans le cyberespace. Puis, le « cyberespace » se définit comme « le milieu complexe découlant de l'interaction des personnes, des logiciels et des services offerts sur Internet au moyen de dispositifs technologiques et de réseaux qui leur sont rattachés, et qui ne présentent aucune forme physique ».

L'Association canadienne des courtiers de fonds mutuels (ACFM) définit la cybersécurité comme un processus qui consiste à protéger l'information en empêchant et en décelant les attaques, les dommages et l'accès non autorisé et en luttant contre eux.

Quelle que soit la définition utilisée, la cybersécurité est un domaine prioritaire pour les entreprises et les organismes de réglementation partout dans le monde en raison des préjudices potentiels que peuvent présenter les menaces aux clients, aux entreprises et au secteur des placements en général. Les menaces à la cybersécurité sont nombreuses et variées et elles évoluent rapidement.

Le présent guide a pour objet de fournir aux membres de l'IFIC une liste des ressources qui sont à leur disposition et qui peuvent être utiles pour élaborer un solide programme de cybersécurité.

CADRE DE TRAVAIL

Toutes les firmes de courtage inscrites sont tenues d'établir, de tenir à jour et d'appliquer des politiques et des procédures qui créent un système de contrôles et de supervision afin d'assurer la conformité avec les lois sur les valeurs mobilières, et de gérer les risques liés à leurs activités conformément aux pratiques commerciales prudentes. Les contrôles de cybersécurité doivent veiller à ce que les réseaux, les ordinateurs, les programmes et les données soient protégés de manière appropriée des attaques, des dommages et de l'accès non autorisé.

Un cadre de cybersécurité efficace est essentiel, car il aidera les firmes à :

- déterminer les biens qui doivent être protégés, de même que les menaces et les risques qui y sont rattachés;

- protéger ces biens à l'aide de mesures de protection appropriées;
- détecter les intrusions, les infractions à la sécurité et l'accès non autorisé;
- intervenir en cas d'événements de cybersécurité potentiels ou réels;
- se remettre d'un événement de cybersécurité.

Un cadre efficace doit comprendre les éléments présentés ci-dessous. Cette liste n'est pas exhaustive; elle représente plutôt une norme minimale qui peut être adaptée en fonction de l'envergure et de la nature des activités de la firme.

Politiques et procédures

Les firmes doivent se doter de politiques et de procédures en matière de cybersécurité. Les politiques et les procédures doivent faire l'objet d'un examen périodique (au moins une fois par année) dans le but de s'assurer qu'elles sont toujours pertinentes et à jour. Les politiques et les procédures doivent traiter de la prévention, de la détection, de la formation et des plans de continuité des activités durant un incident de cybersécurité. Les sujets à aborder comprennent :

- l'utilisation des communications électroniques, notamment les types de renseignements pouvant être recueillis ou transmis par courriel, l'utilisation des systèmes de communication sécurisés et non sécurisés, la vérification des directives des clients transmises par voie électronique et les pratiques des médias sociaux;
- l'utilisation des appareils électroniques (personnels ou fournis par la firme), notamment pour accéder au réseau et aux données de la firme à l'interne et à l'externe;
- la perte ou la destruction des appareils électroniques, y compris les dispositifs de stockage électroniques (p. ex., les clés USB);
- l'utilisation des appareils électroniques publics ou personnels ou des connexions Internet publiques ou personnelles pour accéder à distance au réseau et aux données de la firme, notamment l'accès aux communications avec les clients ou aux renseignements sur les clients;
- la détection des activités internes ou externes non autorisées (p. ex., piratage, hameçonnage, logiciels malveillants);
- la protection des données, notamment le chiffrement des données, le stockage de données et les portails d'information;
- la mise à jour en temps opportun des logiciels, notamment les logiciels antivirus;
- la surveillance et la vérification approfondie des fournisseurs et des prestataires de services externes qui ont accès au réseau et aux données de la firme;
- le signalement à l'échelon supérieur des incidents de cybersécurité et la production de rapports à cet égard.

Formation

Les employés représentent souvent la première ligne de défense en cas de cyberattaque. Pour faire face aux menaces ou aux incidents, la firme doit leur offrir une formation appropriée. En raison de la nature dynamique des cyberactivités, la formation doit être donnée à une fréquence suffisante pour demeurer pertinente, mais pas moins d'une fois par année.

La formation doit être axée sur :

- la reconnaissance des risques;
- la détermination des types de cybermenaces auxquels les employés peuvent être confrontés et les mesures à prendre pour répondre à ces menaces;

- le traitement des renseignements confidentiels de la firme ou des clients;
- l'utilisation de mots de passe forts;
- la protection des appareils électroniques;
- l'identification de cybermenaces réelles ou potentielles ou d'incidents de cybersécurité;
- la détermination du moment et de la manière de signaler les incidents de cybersécurité.

Évaluation des risques

Les firmes doivent effectuer une évaluation périodique des risques en matière de cybersécurité. L'évaluation peut consister à :

- déterminer les biens et les données de la firme qui doivent être protégés;
- déterminer les activités vulnérables de la firme;
- déterminer les conséquences possibles des cybermenaces;
- évaluer les contrôles préventifs et le plan d'intervention en cas d'incidents afin de déterminer si des changements sont nécessaires.

Plan d'intervention en cas d'incidents

Les firmes doivent avoir un plan d'intervention en cas d'incidents qui est documenté et mis à l'essai périodiquement. Le plan d'intervention en cas d'incidents peut comprendre les mesures suivantes :

- déterminer qui est responsable de signaler l'événement de cybersécurité, qui doit être informé (personnes ou groupes) et quels détails doivent être communiqués;
- décrire les divers types de cyberattaques et les procédures à suivre pour mettre fin à l'incident;
- récupérer ou restaurer les données;
- mener une enquête sur l'incident afin de déterminer l'ampleur et la cause des dommages;
- passer en revue et modifier les systèmes, les politiques et les procédures pour empêcher qu'un événement similaire se reproduise.

Fournisseurs et prestataires de services externs

En plus de tenir à jour des politiques et des procédures rigoureuses en matière de vérification et de surveillance des fournisseurs et des prestataires de services externes, les firmes doivent faire signer à ces derniers des accords qui comportent des clauses sur la cybersécurité et le signalement des incidents de cybersécurité.

Assurance

Les firmes doivent passer périodiquement en revue leur couverture d'assurance afin de déterminer si leurs garanties sur la cybersécurité sont suffisantes.

Diffusion de l'information

Les firmes peuvent tirer parti des occasions de diffuser l'information. La diffusion de l'information peut se faire à partir d'un site Web parrainé par un gouvernement ou par l'entremise d'un réseau de pairs de confiance. Cela peut aider à déterminer les faiblesses potentielles et à déceler les menaces dès qu'elles touchent votre firme ou même avant.

Certification en cybersécurité

Le gouvernement du Canada a mis en place un programme de cybercertification pour aider les entreprises canadiennes à se doter d'une sécurité de base. S'inscrivant dans la Stratégie nationale de cybersécurité, ce programme s'adresse aux petites et moyennes entreprises.

CyberSécuritaire Canada est un programme à participation volontaire fondé sur les 13 contrôles de base décrits dans les Contrôles de cybersécurité de base pour les petites et moyennes organisations du Centre canadien pour la cybersécurité. Les entreprises certifiées peuvent utiliser la marque CyberSécuritaire Canada pendant une période de deux ans.

ANNEXE A – RESSOURCES EN MATIÈRE DE CYBERSÉCURITÉ DES ORGANISMES DE RÉGLEMENTATION

ORGANISMES DE RÉGLEMENTATION CANADIENS

Avis 11-332 du personnel des ACVM sur la cybersécurité
https://www.osc.gov.on.ca/documents/en/Securities-Category1/sn_20160927_11-332-cyber-security.pdf

Avis 33-321 du personnel des ACVM sur la cybersécurité et les médias sociaux
http://www.osc.gov.on.ca/documents/en/Securities-Category3/csa_20171019_33-321_cyber-security-and-social-media.pdf

Guide de pratiques exemplaires en matière de cybersécurité à l'intention des courtiers membres de l'OCRCVM
https://www.ocrcvm.ca/industry/Documents/CybersecurityBestPracticesGuide_fr.pdf

Gestion des cyberincidents – Guide de planification à l'intention des courtiers membres de l'OCRCVM
https://www.ocrcvm.ca/industry/Documents/CyberIncidentManagementPlanningGuide_fr.pdf

Bulletin 0690-C de l'Association canadienne des courtiers de fonds mutuels (ACFM) sur la cybersécurité
http://www.mfda.ca/regulation/bulletins16/Bulletin0690-C.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

Signalement des incidents liés à la technologie et à la cybersécurité du Bureau du surintendant des institutions financières (BSIF)
http://www.osfi-bsif.gc.ca/fra/fi-if/rg-ro/gdn-ort/adv-prv/Pages/TCSIR.aspx

ORGANISMES DE RÉGLEMENTATION INTERNATIONAUX

Guidance on Cyber Resilience for Financial Market Infrastructures du CPIM et de l'OICV (en anglais)
http://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf

Site Web sur la cyberrésilience de la Financial Conduct Authority (FCA)
https://www.fca.org.uk/firms/cyber-resilience

Report on Selected Cybersecurity Practices – 2018 de la Financial Industry Regulatory Authority (FINRA) (en anglais)
https://www.finra.org/sites/default/files/Cybersecurity_Report_2018.pdf

Report on Cybersecurity Practices de la Financial Industry Regulatory Authority (FINRA) (en anglais)
https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf

Liste de vérification en matière de cybersécurité de la Financial Industry Regulatory Authority (FINRA) (en anglais)
http://www.finra.org/industry/small-firm-cybersecurity-checklist

Rapport de l'OICV sur la cybersécurité dans les marchés des valeurs mobilières (en anglais)
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 (en anglais)
http://www.iosco.org/library/pubdocs/pdf/IOSCOPD522.pdf

Liste de vérification en matière de cybersécurité de la North American Securities Administrators Association (NASAA) (en anglais)
http://nasaa.cdn.s3.amazonaws.com/wp-content/uploads/2011/08/NASAA-Cybersecurity-Checklist.pdf

Observations sur les examens relatifs à la cybersécurité de la Securities and Exchange Commission (SEC) (en anglais)
https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf

Ressources en matière de cybersécurité de la Securities Industry and Financial Markets Association (SIFMA)
https://www.sifma.org/cybersecurity-resources/

ANNEXE B – AUTRES RESSOURCES EN MATIÈRE DE CYBERSÉCURITÉ

Contrôles de cybersécurité de base pour les petites et moyennes organisations
https://cyber.gc.ca/sites/default/files/publications/Contr%C3%B4les%20de%20cybers%C3%A9curit%C3%A9%20de%20base%20pour%20les%20petites%20et%20moyennes%20organisations%20v1.1_0.pdf

Site Web sur la sécurité de l'information de la Colombie-Britannique
https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security

Alertes et avis de cybersécurité de la Colombie-Britannique
https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/cyber-security-alerts-notifications

Centre canadien pour la cybersécurité
https://cyber.gc.ca/

Center for Internet Security
https://www.cisecurity.org/

Questionnaire d'évaluation (v3.0.1) dans le cadre de la Consensus Assessments Initiative de la Cloud Security Alliance (en anglais)
https://downloads.cloudsecurityalliance.org/initiatives/cai/caiq-v3.0.1.zip

CyberSécuritaire Canada
https://www.ic.gc.ca/eic/site/137.nsf/fra/h_00000.html

Renforcer la résilience des infrastructures essentielles du Canada aux risques internes
https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/nhncng-crtcl-nfrstrctr/index-fr.aspx

Outil d'évaluation de la cybersécurité du Federal Financial Institutions Examination Council (FFIEC) (en anglais)
https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf

Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices du Financial Stability Board (en anglais)
http://www.fsb.org/wp-content/uploads/P131017-1.pdf

Lexique sur la cybersécurité (en anglais) du Financial Stability Board
http://www.fsb.org/wp-content/uploads/P121118-1.pdf

National Cyber Security Centre du GCHQ
https://www.ncsc.gov.uk/

Plan de gestion des événements de cybersécurité du gouvernement du Canada (PGEC GC) 2018
https://www.canada.ca/fr/secretariat-conseil-tresor/services/acces-information-protection-reseignements-personnels/gestion-securite-identite/plan-gestion-evenements-cybersecurite-gouvernement-canada.html

InfraGard
https://www.infragard.org/

IIFA Cybersecurity Program Basics
https://www.iifa.ca/files/1571405868_IIFA%20Cybersecurity%20Program%20Basics.pdf

Control Objectives for Information and Related Technology (COBIT) de l'Information Systems Audit and Control Association (ISACA)
http://www.isaca.org/cobit/pages/default.aspx

National Institute of Standards and Technology
https://www.nist.gov/topics/cybersecurity

Framework for Improving Critical Infrastructure Cybersecurity de la National Institute of Standards and Technology
https://doi.org/10.6028/NIST.CSWP.04162018

Groupe national de coordination contre la cybercriminalité (GNCC)
http://www.rcmp-grc.gc.ca/fr/groupe-national-coordination-cybercriminalite-gncc

SANS Top 20 Critical Security Controls
http://www.cisecurity.org/critical-controls/

Questionnaire d'évaluation des tiers fournisseurs de l'Université de la Colombie-Britannique (en anglais)
https://it.ubc.ca/sites/it.ubc.ca/files/3rd%20Party%20Outsourcing%20Information%20Security%20Assessment%20Questionnaire%20V1.4.xlsx