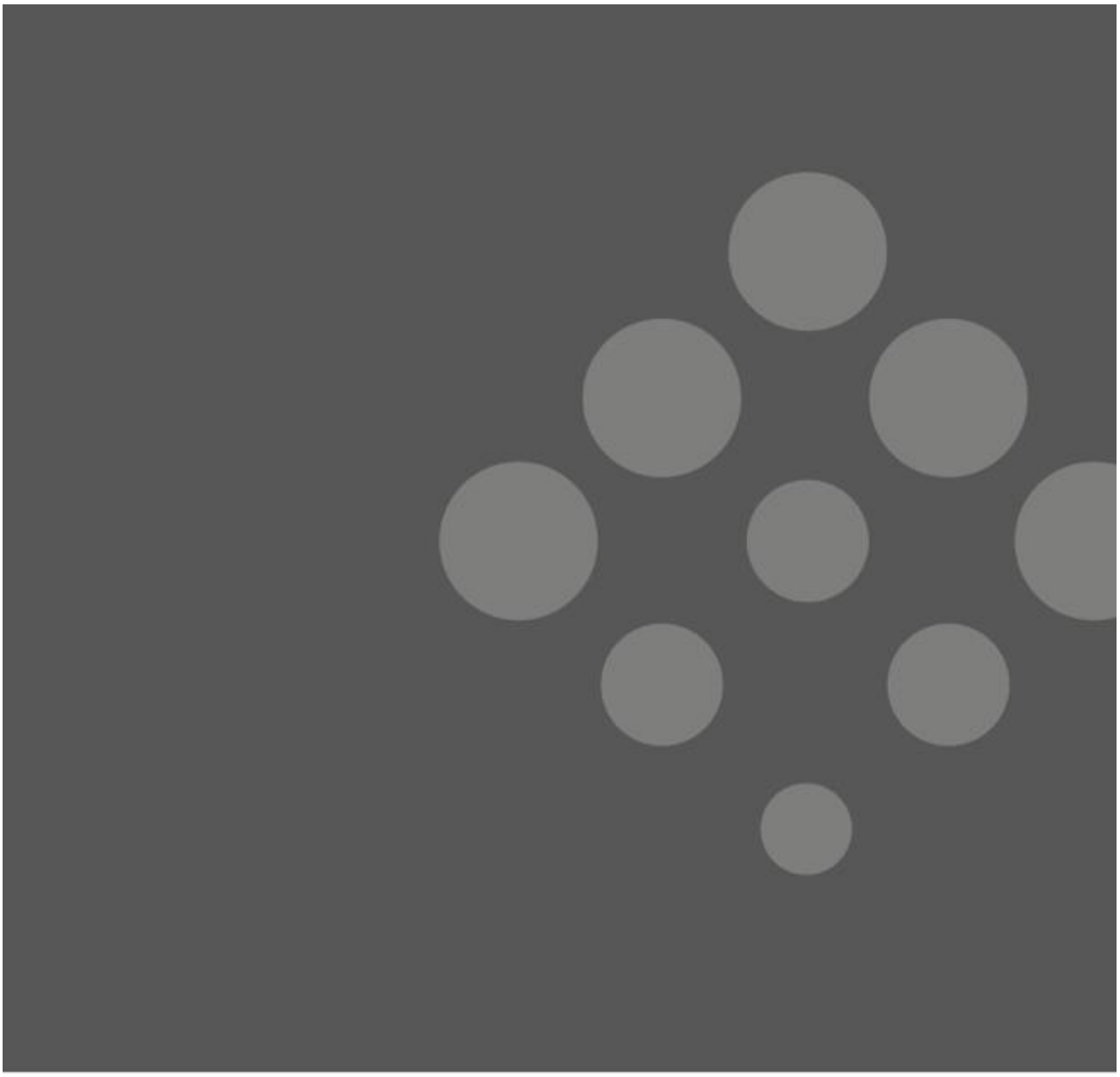


Guide de cybergouvernance de l'OCRCVM

31 janvier 2020

IIROC OCRCVM
Investment Industry Regulatory Organization of Canada
Organisme canadien de réglementation du commerce des valeurs mobilières

juno risk solutions

1. INTRODUCTION 4
1.1 STRUCTURE DU DOCUMENT 4
1.2 LE DÉFI 4
1.3 L'APPROCHE 4

2. ENVIRONNEMENT DES MENACES 6
2.1 QU'EST-CE QUI CONSTITUE UNE MENACE? 6
2.2 SOURCES DE MENACE 6
Menaces internes 6
Crime organisé 8
Espionnage étranger et espionnage industriel 8
2.3 SAVOIR-FAIRE HUMAIN 10
2.4 CYBERSAVOIR-FAIRE 11

3. POLITIQUE DE SÉCURITÉ ET GOUVERNANCE DES PROGRAMMES 13
3.1 LEADERSHIP ET OBLIGATION FIDUCIAIRE 13
3.2 PRINCIPAUX ÉLÉMENTS DU PROGRAMME DE CYBERSÉCURITÉ 14
Tenue d'un inventaire des actifs 14
Réalisation d'évaluations des risques 14
Élaboration et maintien d'un programme écrit de sécurité de l'information 14
Élaboration et application d'une politique de sécurité de l'information 14
Formation et sensibilisation 15
Gestion des risques que présentent les fournisseurs 15
3.3 ASSURANCE CONTRE LES CYBERRISQUES 16
3.4 PRINCIPAUX FACTEURS JURIDIQUES 18
3.5 POLITIQUES ET PROCÉDURES 19

4. CADRE OPÉRATIONNEL 21
4.1 CADRE DE CYBERSÉCURITÉ DU NIST 21
4.2 POURQUOI SE FIER AU NIST? 22
4.3 APPROCHE PROGRESSIVE 22
4.4 ÉVALUATION DES COÛTS, DES DIFFICULTÉS ET DE L'ÉCHÉANCIER 23
4.5 DESCRIPTION DES PROFILS 23

5. DIRECTIVES POUR LA MISE EN ŒUVRE D'UN PROGRAMME OPÉRATIONNEL 26
5.1 DILIGENCE RAISONNABLE ET DEVOIR DE DILIGENCE 27
5.2 ÉTAT DE PRÉPARATION 28
Intervention en cas d'incident 28
Copies de sauvegarde 28
Cyberexercices de simulation 28
Planification de la poursuite des activités 29
5.3 ÉVALUATION DES MENACES ET DES VULNÉRABILITÉS 30
5.4 ÉLABORATION D'UN PROGRAMME COMPLET 31

6. RECOMMANDATIONS DE PRATIQUES EXEMPLAIRES 32
6.1 ENQUÊTE DE SÉCURITÉ SUR LE PERSONNEL ET MENACES INTERNES 32
6.2 SÉCURITÉ PHYSIQUE ET ENVIRONNEMENTALE 34
6.3 SENSIBILISATION À LA CYBERSÉCURITÉ ET FORMATION 35
6.5 SÉCURITÉ DU RÉSEAU 37
6.6 SÉCURITÉ DES RÉSEAUX SANS FIL 38
6.7 ACCÈS À DISTANCE 39
6.8 SÉCURITÉ DES POINTS TERMINAUX 40
6.9 PROTECTION DES SYSTÈMES D'INFORMATION 41
6.10 APPORTEZ VOTRE ÉQUIPEMENT PERSONNEL DE COMMUNICATION 42

6.11 GESTION DES APPAREILS MOBILES 43
6.12 SAUVEGARDE ET REPRISE DES ACTIVITÉS 43
6.13 GESTION DES COMPTES D'UTILISATEUR ET CONTRÔLE DE L'ACCÈS 44
6.14 GESTION DES ACTIFS 45

7. INTERVENTION EN CAS D'INCIDENT ***46***
7.1 TERMES CLÉS 46
7.2 MODÈLE D'INTERVENTION EN CAS D'INCIDENT 46
7.3 STRUCTURE MODULAIRE 47
7.4 GESTION PAR OBJECTIFS 47
7.5 PLAN D'ACTION EN CAS DE CYBERINCIDENT 48
7.6 ÉVENTAIL DE COMMANDEMENT GÉRABLE 48
7.7 EMPLACEMENT DES INSTALLATIONS DÉSIGNÉES EN CAS D'INCIDENT 49
7.8 GESTION EXHAUSTIVE DES RESSOURCES 49
7.9 COMMUNICATIONS INTÉGRÉES 49
7.10 ÉTABLISSEMENT DU COMMANDEMENT ET TRANSFERT DE COMMANDEMENT 49
7.11 CHAÎNE DE COMMANDEMENT 49
7.12 DÉPLOIEMENT 49
7.13 GESTION DE L'INFORMATION ET DES RENSEIGNEMENTS 50

8. ORGANISATION ET OPÉRATIONS LORS D'UNE INTERVENTION EN CAS D'INCIDENT ***51***
8.1 CINQ PHASES PRINCIPALES DU PROCESSUS DE PLANIFICATION 52
Comprendre la situation 52
Établir les objectifs en cas d'incident et adopter une stratégie 52
Élaborer un plan 52
Préparer et distribuer le plan 52
Exécuter, évaluer et revoir le plan 53

9. ÉCHANGE D'INFORMATION ET SIGNALEMENT DES INFRACTIONS ***54***
9.1 AVIS D'ATTEINTE À LA VIE PRIVÉE 54
9.2 ÉCHANGE D'INFORMATION 54
9.3 GESTION DES RISQUES LIÉS AUX FOURNISSEURS ET À L'EXTERNALISATION 54
9.4 INFONUAGIQUE 56
9.5 FOURNISSEURS DE SERVICES GÉRÉS 57
9.6 OUTILS COMPLETS DE BUREAUTIQUE ET DE COLLABORATION 58
9.7 GOUVERNANCE HYBRIDE 59

1. INTRODUCTION

Le Guide de cybergouvernance de l'OCRCVM fournit aux courtiers membres de l'OCRCVM (les **courtiers membres**) des indications claires sur la façon optimale de promouvoir, de mettre en œuvre et de gérer un programme de cybersécurité. Le présent document devrait être consulté conjointement avec le Guide de pratiques exemplaires en matière de cybersécurité de 2015 de l'OCRCVM, étant donné qu'il reprend l'information de ce guide et y apporte des précisions. Le présent guide témoigne de l'expérience acquise par l'OCRCVM et par les courtiers membres dans le cadre de l'élaboration et de la mise en œuvre de programmes visant à contrer les cybermenaces.

1.1 STRUCTURE DU DOCUMENT

Le document est structuré de manière à aider les courtiers membres à comprendre les menaces actuelles que posent des cybercriminels, des services du renseignement étrangers hostiles et leurs propres employés et parties intéressées du milieu des affaires. Les courtiers membres sont encouragés à demeurer vigilants face aux changements qui surviennent dans l'environnement des menaces, et se méfier entre autres des nouvelles combines utilisées pour pirater les systèmes, exploiter l'information ou accéder aux fonds.

1.2 LE DÉFI

La meilleure façon de caractériser le défi que posent les pirates informatiques pour les courtiers membres est dans le contexte de deux modèles d'affaires concurrentiels. Les courtiers membres du secteur des valeurs mobilières comptent sur un écosystème de clients, de systèmes internes, d'employés et de relations avec des tiers pour offrir des services à leurs clients et générer un revenu. Pour générer un revenu, les cybercriminels adoptent un modèle d'affaires qui suppose l'infiltration de votre modèle d'affaires. Habituellement, les cyberattaques sont le travail de criminels organisés qui emploient leurs propres partenaires tiers chargés d'accéder aux logiciels malveillants et aux services d'attaques d'hameçonnage, d'effectuer les paiements de rançongiciel avec de la cryptomonnaie et de trouver leur prochaine cible. Le paiement à ces fournisseurs de services illicites est conditionnel à l'infiltration réussie des sociétés et à l'accès aux fonds. De la même façon que le commerce de la drogue est devenu une multinationale intégrée, le crime organisé est passé à la cybercriminalité, soit à des activités criminelles de grande valeur comportant peu de risques.

1.3 L'APPROCHE

Le présent rapport vise à présenter aux courtiers membres de l'OCRCVM une vision globale de la cybersécurité et d'apporter des précisions sur les pratiques exemplaires à cet égard.

La **section 2** examine l'actuel environnement opérationnel des menaces auquel font face les courtiers membres et met l'accent sur le savoir-faire humain et le cybersavoir-faire.

La **section 3** fournit des indications sur la dimension juridique d'une cybergouvernance judicieuse et aborde la nature complexe et évolutive du marché de la cyberassurance.

La **section 4** présente le cadre de cybersécurité du NIST et l'idée que certaines mesures de protection devraient être prioritaires selon les capacités du courtier membre, la nature de la menace et les services financiers qu'il offre.

La **section 5** propose un cadre de gouvernance permettant de prendre en considération les mesures de protection du NIST et de prioriser leur mise en œuvre. Le but de ce classement relatif est d'insuffler un certain leadership au courtier membre, en lui donnant une idée de l'avantage relatif qu'offre un investissement dans la sécurité.

La **section 6** formule une série de recommandations pour que la sécurité soit basée sur des pratiques exemplaires établies.

Les **sections 7** et **8** donnent un aperçu des principaux facteurs à examiner lors d'une intervention en cas de cyberincident. Il est notamment question de la nature des événements déclencheurs, de la relation nécessaire entre les ressources internes d'un courtier membre et celles des fournisseurs externes pour une intervention, et de la meilleure façon d'harmoniser les besoins du courtier membre au moment de souscrire une protection suffisante auprès d'un fournisseur de cyberassurance.

Pour finir, la **section 9** traite de l'importance de l'échange d'information et du signalement des infractions.

2. ENVIRONNEMENT DES MENACES

2.1 QU'EST-CE QUI CONSTITUE UNE MENACE?

Les cybermenaces présentent un risque pour les courtiers membres de l'OCRCVM. « Cybermenace » est un terme générique qui souvent ne permet pas de comprendre les mesures correctives à prendre contre les risques qui existent. On recommande que le courtier membre s'efforce d'abord de personnifier la menace précise qui plane sur sa propre entreprise. Demandez-vous quels renseignements utiles ou quel accès détient votre société, comment ceux-ci peuvent être exploités à des fins criminelles et quel pourrait être le type de criminel ou la source de menace cherchant à les exploiter. Lorsque vous avez une idée des criminels ou des sources de menace qui pourraient accéder à vos systèmes et de la façon dont ils s'y prendraient, il vous est alors plus facile d'examiner les vulnérabilités de votre société et de prioriser leur atténuation.

Une menace est une source qui a les *capacités*, *l'intention* et l'*occasion* de causer des dommages. Ces trois caractéristiques sont nécessaires pour qu'une source représente une menace. La présente section aborde le sujet des sources de menace possibles et la façon dont celles-ci peuvent causer un préjudice en ayant recours au savoir-faire humain et au cybersavoir-faire. Le terme savoir-faire est utilisé dans la présente section pour désigner les méthodes et les moyens employés par les sources de menace pour accéder aux systèmes et à l'information. Le cybersavoir-faire continue de se perfectionner et imite les avancées en matière de contrôles de sécurité. L'objectif de la présente section est d'énoncer les concepts clés qui favoriseront un meilleur examen des pratiques exemplaires relatives aux contrôles de sécurité proposées dans les sections suivantes.

2.2 SOURCES DE MENACE

La présente section examine les nombreuses sources de menace qui représentent une menace interne pour l'OCRCVM et ses courtiers membres. L'expérience a montré que le fait d'illustrer la nature de la menace en faisant référence aux expériences vécues par d'autres aide l'organisation à prendre des décisions plus efficaces en ce qui concerne la conception des programmes de sécurité.

Menaces internes

Une menace interne est définie comme [traduction] « un employé actuel ou un ancien employé, un sous-traitant ou un partenaire d'affaires qui a ou avait un accès autorisé au réseau, à un système ou aux données d'une organisation, et qui a délibérément mal utilisé cet accès ou outrepassé ses droits d'accès, et a ainsi porté atteinte à la confidentialité, à l'intégrité ou à la disponibilité des renseignements ou des systèmes informatiques de l'organisation »[1]. Les menaces internes peuvent se manifester sous la forme de menaces à la sécurité liées à des activités d'espionnage criminelles ou d'États-nations, ou sous la forme d'une communication non autorisée de renseignements sensibles.

[1] Université Carnegie Mellon. *The CERT Insider Threat Centre* (en anglais seulement), 2017.

Edward Snowden, cet ancien sous-traitant de la National Security Agency, a volé des millions de documents classifiés pour ensuite les publier; il s'agit de l'incident le plus important et le plus préjudiciable de l'histoire des États-Unis sur le plan de la publication de documents classifiés. Le House Select Committee on Intelligence Report (rapport du comité spécial du renseignement de la Chambre), publié en version expurgée en décembre 2016, met en lumière un schème de comportement de la part d'Edward Snowden : de fausses déclarations sur des documents d'emploi, un certain mépris à l'égard de l'autorité et une conduite dépassant ses pouvoirs qui, en rétrospective, font penser clairement à des problèmes de fiabilité[2]. Le vol et la publication de ces documents classifiés étaient une autre manifestation de ces traits de comportement.

L'Office of the Comptroller of the Currency des États-Unis a indiqué au Congrès, à l'automne 2015, qu'un ancien employé avait téléchargé plus de 10 000 fichiers sur deux clés USB, qu'il avait prises avec lui avant de prendre sa retraite[3]. La Federal Deposit Insurance Corporation des États-Unis a informé le Congrès de sept infractions qui ont eu lieu au moment où des employés ont quitté l'agence, prenant avec eux des données sensibles. Ces incidents ont possiblement fait en sorte que les renseignements confidentiels de près de 160 000 Américains aient été rendus publics[4].

Les employés qui bénéficient de privilèges accrus représentent une menace particulièrement importante. Le réseau du Chemin de fer Canadien Pacifique (CFCP) a été la proie d'un acte de sabotage par un employé qui a été licencié[5]. À la fin de 2015, l'administrateur d'un système informatique, Christopher Grupe, a été suspendu pendant 12 jours pour insubordination. À son retour au travail, le CFCP a décidé de le licencier, puis a accepté de le laisser donner sa démission à la place. Alors qu'il avait encore accès au réseau, Christopher Grupe s'est servi de ses identifiants d'accès à distance pour supprimer les droits d'accès d'administrateur de certains comptes, supprimer du réseau d'importants fichiers et modifier certains mots de passe de sorte que d'autres employés n'aient plus accès au réseau. Il a aussi supprimé tous les fichiers montrant ce qu'il avait fait. Les dommages étaient tellement considérables que le réseau a dû être rétabli.

Une menace interne provient soit d'un membre du personnel, soit d'un invité autorisé à entrer dans l'établissement, mais qui contrevient aux normes et au code de conduite de l'organisation. L'OCRCVM et ses courtiers membres emploient directement des milliers d'employés, mais aussi un certain nombre de sous-traitants temporaires, d'étudiants et d'employés nommés pour une période déterminée. Cela crée une main-d'œuvre diversifiée et souvent transitoire qui a accès à leurs installations.

---

[2] Chambre des représentants des États-Unis. *Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden* (en anglais seulement), 2016.
[3] The Wall Street Journal. *U.S. Bank Regulator Notifies Congress of Major Data Security Breach* (en anglais seulement), 28 octobre 2016.
[4] Ibid.
[5] Département de la Justice des États-Unis. *Former Employee of Transcontinental Railway Company Found Guilty of Damaging Ex-Employer's Computer Network* (en anglais seulement), 10 octobre 2017.

Crime organisé

Le crime organisé représente une menace grave à long terme pour la société, l'économie et les institutions canadiennes, et pour la qualité de vie de la population canadienne. Les groupes transnationaux de crime organisé ont atteint récemment le même niveau de sophistication que les grands organismes de renseignement des États-nations. À l'heure actuelle, les cyberattaques comportent peu de risques pour ceux qui ont les moyens de concevoir et d'exécuter des stratagèmes criminels, et elles leur offrent des possibilités très satisfaisantes. Fraude, vol d'identité et extorsion sont trois manifestations génériques de la cybercriminalité.

Le marché de la collecte de renseignements et de l'exploitation criminelle de l'information a rapidement pris de la maturité au cours des dernières années. Il est faux de penser que les organisations sont protégées simplement parce que la nature granulaire, non structurée ou apparemment inintéressante de leurs données rend leur exploitation improbable. Les pirates informatiques offrent leurs services à des criminels qui savent comment exploiter l'information interne et qui ont l'intention d'user de stratagèmes pour faire un profit financier.

Les criminels doués en finance qui savent comment utiliser des renseignements exclusifs sont connus pour avoir recours à des pirates informatiques pour accéder aux renseignements qui leur permettront de peaufiner leurs stratagèmes. En 2014, 76 millions de comptes commerciaux et 7 millions de comptes de petites entreprises ont été volés à la JP Morgan Chase & Co.[6]. Dans le document d'inculpation de trois personnes, le Federal Bureau of Investigation a expliqué que les co-comploteurs cherchaient à parfaire un stratagème classique de manipulation d'actions de type « pump-and-dump » et ont retenu les services d'un pirate informatique en vue de pirater un certain nombre d'institutions financières et d'obtenir les courriels de cibles potentielles vantant leurs actions de choix. Le stratagème a prétendument rapporté aux comploteurs des millions de dollars.

Espionnage étranger et espionnage industriel

En décembre 2018, David Vigneault, le directeur du Service canadien du renseignement de sécurité (SCRS), a déclaré que la plus grande menace à la prospérité du Canada et aux intérêts nationaux était l'ingérence étrangère et l'espionnage étranger[7]. M. Vigneault a indiqué que des services du renseignement étrangers hostiles ou des personnes travaillant avec le soutien tacite ou explicite d'États étrangers recueillaient activement, par des moyens clandestins, des renseignements d'ordre politique, économique, commercial ou militaire au Canada.

Certains États étrangers, en particulier la Chine et la Russie, représentent une menace importante sur le plan du renseignement pour les institutions gouvernementales canadiennes et le secteur privé canadien. Une étude publiée récemment, à laquelle ont collaboré des universités étrangères et l'armée chinoise, montre que les recherches universitaires peuvent être l'occasion de recueillir des données sensibles et de nouer des relations avec des chefs de file étrangers de la

[6] Wired. *Four Indicted in Massive JP Morgan Chase Hack* (en anglais seulement), 10 novembre 2015.
[7] Gouvernement du Canada. *Allocution de David Vigneault au Economic Club of Canada*, 4 décembre 2018.

recherche[8]. Des dizaines de scientifiques de l'Armée populaire de libération (APL) ont caché leurs affiliations militaires pour se rendre dans des pays du Groupe des cinq (Canada, Australie, Nouvelle-Zélande, Royaume-Uni et États-Unis) et de l'Union européenne. En outre, au cours de la dernière décennie, l'armée chinoise a parrainé les déplacements de plus de 2 500 scientifiques. Des 10 premières universités autres que les universités chinoises qui ont été choisies pour une collaboration avec l'APL, l'Université de Waterloo figure au 4e rang, et l'Université de Toronto et l'Université McGill, aux 9e et 10e rangs, respectivement.

En 2017, le Congrès national du peuple chinois a adopté la *National Intelligence Law* (loi sur le renseignement national) qui prévoit que tous les citoyens chinois ont le devoir de coopérer avec les organismes de sécurité et de renseignement du pays[9]. Cette loi sanctionne la cooptation de représentants d'autres organismes gouvernementaux chinois et la coopération obligatoire d'autres citoyens de la République populaire de Chine. Cela suppose que des représentants de ministères apparemment inoffensifs du gouvernement chinois peuvent aussi représenter une menace sur le plan de la collecte de renseignements.

Des groupes du crime organisé et des services du renseignement étrangers utilisent les médias sociaux pour repérer les personnes qui ont accès à des renseignements pertinents. L'utilisation massive de faux profils pour d'abord entrer en contact avec des personnes ciblées, puis pour communiquer avec elles, est l'une des tactiques employées. Les services du renseignement allemands et français ont mis en garde leurs citoyens contre les services du renseignement chinois qui utilisent massivement LinkedIn pour repérer des personnes ayant accès à des renseignements d'intérêt pour le gouvernement chinois. L'organisme de renseignement national de l'Allemagne affirme que la Chine s'est servie de LinkedIn pour cibler au moins 10 000 personnes[10]. Le gouvernement français a indiqué que des espions chinois ont communiqué, par l'entremise de LinkedIn, avec au moins 4 000 fonctionnaires, scientifiques et hauts dirigeants français occupant un rôle prépondérant[11]. De ceux-ci, 2 300 travaillent dans le secteur public, et 1 700 occupent un poste au sein de l'industrie française. Le rapport du service du renseignement français indiquait que les personnes ciblées provenaient de presque tous les secteurs de l'industrie et de l'administration de l'État. Elles sont entrées en relation en ligne avec des espions chinois qui utilisaient de fausses identités et qui se présentaient comme des chasseurs de têtes pour des sociétés chinoises, des chercheurs de centres d'études et de recherches ou des consultants pour d'importantes sociétés. En règle générale, les personnes ciblées étaient ensuite invitées en Chine à des conférences ou à des symposiums de recherche, tous frais compris, ou un travail rémunéré de consultant leur était offert.

Des agents du renseignement hostiles cherchent des personnes aux prises avec des problèmes personnels pour s'en servir comme éventuelles sources de renseignements. La volonté d'une

[8] Australian Strategic Policy Institute. *Picking flowers, making honey* (en anglais seulement), 30 octobre 2018.
[9] Gouvernement du Canada. *La Loi sur le renseignement national de la Chine et l'avenir des rivalités avec le pays sur le plan du renseignement*.
[10] BBC News. *German spy agency warns of Chinese LinkedIn espionage* (en anglais seulement), 10 décembre 2017.
[11] Le Figaro. *Les révélations du Figaro sur le programme d'espionnage chinois qui vise la France*, octobre 2018.

personne de se livrer à des activités d'espionnage contre son employeur s'explique souvent par une crise personnelle accompagnée de pressions externes définies. En octobre 2012, l'enseigne de vaisseau de 1re classe Jeffery Paul Delisle a plaidé coupable à des accusations d'espionnage pour la Russie. Il occupait alors le poste d'agent du renseignement pour la Marine royale canadienne dans des installations de haute sécurité à Halifax[12]. Il avait surpris sa femme en train de le tromper et connaissait de grandes difficultés financières. Il avait alors informé son supérieur de ses problèmes, mais ce dernier n'en avait pas tenu compte et ne lui avait pas apporté le soutien organisationnel approprié. Le service du renseignement militaire russe s'est servi de M. Delisle pour obtenir des renseignements de 2007 à 2012, avant que celui-ci ne soit arrêté. Au cours de cette période, il a fait sortir clandestinement de grandes quantités de renseignements hautement classifiés à l'aide d'une clé USB. Cette infraction est considérée comme l'une des pires atteintes à la sécurité des services du renseignement occidentaux depuis la fin de la Guerre froide. Cette affaire souligne la volonté des services du renseignement étrangers actifs au Canada de recruter des représentants du gouvernement canadien qui occupent des postes de confiance et qui ont accès à des renseignements d'intérêt pour leur pays.

2.3 SAVOIR-FAIRE HUMAIN

Le savoir-faire témoigne de la « façon » dont les systèmes et l'accès aux personnes peuvent être exploités à des fins criminelles. Nous proposons l'analyse du savoir-faire ci-après pour mettre en contexte la section sur les contrôles de sécurité qui suit. L'objectif est de sensibiliser le lecteur aux façons dont les systèmes et les gens peuvent créer des vulnérabilités en matière de sécurité.

Extorsion

- L'extorsion est une pratique qui consiste à obtenir quelque chose de valeur par la force ou la menace. Comme les employés et les dirigeants sont de plus en plus branchés et ont de plus en plus de comptes sur les médias sociaux, les sources de menace ont accès à une plus grande quantité de renseignements, qu'elles peuvent utiliser contre le personnel pour obtenir des renseignements sensibles, accéder à des systèmes ou influencer la prise de décisions.

Contrôle de l'accès

- L'accès périmétrique peut être obtenu, ce qui comprend l'accès initial aux installations et les contrôles de sécurité internes entre les zones de sécurité. Les criminels profitent de la proximité des réseaux pour y accéder clandestinement.

Contrôle des visiteurs

- Dans tout milieu professionnel, des visiteurs de l'extérieur doivent accéder aux installations. Le contrôle efficace des visiteurs peut accroître le risque d'accès non autorisé au réseau et permettre d'identifier les parties impliquées durant l'analyse réalisée après un incident.

[12] The Globe and Mail. *Naval intelligence officer sold military secrets to Russia for $3,000 a month* (en anglais seulement), publié le 10 octobre 2012, mis à jour le 9 mai 2018.

Sous-traitants

- Les sous-traitants peuvent causer une série de vulnérabilités en matière de sécurité. Ils sont généralement présents pendant un certain temps seulement, mais ils se font souvent accorder un accès considérable aux renseignements sensibles. Il peut être difficile de garder le contrôle des renseignements après la résiliation de leurs contrats, particulièrement si les données ne sont pas conservées dans des systèmes internes.

Détection de talents

- Lorsqu'elles cherchent des employés à exploiter, les sources de menace cherchent d'abord à trouver des personnes qui ont accès à des renseignements pertinents. Il peut s'agir de personnes qui occupent un poste en particulier ou de personnes qui, en raison de leur image publique, possèdent ces connaissances.

Subtilisation de renseignements

- La subtilisation de renseignements est une technique utilisée pour recueillir discrètement des renseignements. Elle s'effectue habituellement durant une conversation qui a un objectif bien précis, celui d'obtenir des renseignements factuels difficilement accessibles sans éveiller de soupçons. La conversation n'est généralement pas menaçante, elle est facile à déguiser et à nier, et elle est efficace.

2.4 CYBERSAVOIR-FAIRE

Hameçonnage

- L'hameçonnage est le fait de tenter d'accéder frauduleusement à des réseaux ou à des données en se faisant passer pour une entité de confiance dans une communication électronique. Normalement, on demande à une personne de cliquer sur un lien dans un courriel, ce qui permet d'installer un logiciel malveillant sur l'ordinateur ou de demander à la personne de fournir ses données d'ouverture de session. L'hameçonnage demeure la plus grande vulnérabilité pour la plupart des organisations, puisqu'il ne faut qu'un seul courriel d'hameçonnage réussi pour fournir l'accès nécessaire au réseau.

Élévation des privilèges

- L'élévation des privilèges est le processus qui consiste à exploiter un défaut de conception ou une erreur de configuration d'un système d'exploitation, d'une application logicielle ou d'une autre ressource du réseau et qui permet à un pirate informatique de commettre un acte qu'il n'est pas autorisé à poser. Les criminels qui accèdent initialement au réseau par hameçonnage cherchent ensuite souvent à accroître leurs privilèges pour exploiter davantage leur tremplin initial.

Perte de données par inadvertance

- La perte de données par inadvertance est le résultat de la suppression accidentelle d'un fichier ou d'un programme, d'une erreur de séquencement des données sur un support de stockage, d'erreurs administratives ou de l'incapacité

à lire un fichier dans un format inconnu. Bien que la présente section soit axée sur les menaces intentionnelles de criminels ou d'espions, les erreurs par inadvertance du personnel peuvent aussi être très dangereuses.

Cyberattaque contre la chaîne d'approvisionnement

- Une cyberattaque contre la chaîne d'approvisionnement porte préjudice à l'organisation en ciblant initialement les éléments moins sécurisés de son infrastructure réseau. Durant l'examen des programmes de sécurité, il est essentiel de tenir compte non seulement des systèmes exploités par la société, mais également de ceux de son réseau élargi de tiers fournisseurs.

Rançongiciel

- Le rançongiciel est un code malveillant qui bloque l'accès aux fichiers ou aux données d'un système à moins qu'une rançon ne soit payée. Dans bien des cas, le pirate peut également menacer de publier les données de la victime. Le rançongiciel est une technique répandue aujourd'hui, et tant les ordinateurs familiaux que les ordinateurs des gouvernements sont ciblés.

DDOS

- Une attaque par déni de service distribué (DDOS) est une cyberattaque dans le cadre de laquelle le pirate cherche à empêcher les utilisateurs autorisés à utiliser les réseaux ou les services, en inondant de requêtes superflues les machines ciblées afin de surcharger le système et d'empêcher le traitement des requêtes légitimes.

3. POLITIQUE DE SÉCURITÉ ET GOUVERNANCE DES PROGRAMMES

3.1 LEADERSHIP ET OBLIGATION FIDUCIAIRE

En vertu des lois canadiennes, les actionnaires élisent les membres d'un conseil d'administration (le **conseil**) qui est chargé de surveiller et de gérer les activités et affaires de la société. Les membres du conseil ont une obligation fiduciaire envers la société et sont tenus de faire preuve de la diligence requise, d'agir de bonne foi et de posséder les compétences nécessaires pour agir avec soin, diligence et jugement en ce qui concerne les activités commerciales de la société. Sur le plan de la cybersécurité, plus particulièrement, les membres du conseil doivent assurer la surveillance du programme de sécurité de la société.

Le manquement des membres du conseil à leur obligation d'effectuer une surveillance efficace du programme de cybersécurité de la société peut compromettre la société et ses actionnaires, et potentiellement leur faire porter la responsabilité. Dans l'éventualité d'une brèche de sécurité, le conseil de la société doit s'attendre à ce que ses fonctions soient examinées à la loupe.

Voici une liste des mesures que peut mettre en place un conseil afin d'exercer ses responsabilités de surveillance en matière de cybersécurité et en cas d'atteinte à la protection des données :

- Veiller à ce que les membres du conseil discutent régulièrement de l'état de préparation de la société en cas de problèmes de cybersécurité et de protection des données lors des réunions du conseil;
- Rédiger après chaque réunion du conseil un procès-verbal précisant les tâches de sécurité qui ont été assignées et leur état d'avancement;
- Déléguer le contrôle des mesures de cybersécurité et des activités de protection des données à un comité du conseil;
- Demander un audit des systèmes de cybersécurité de la société ainsi que des recommandations quant aux améliorations prioritaires;
- Superviser le programme de cybersécurité de la direction en s'assurant qu'il comprend les politiques et les programmes pertinents, et qu'il s'aligne sur les normes de cybersécurité applicables;
- Superviser les efforts que déploie la direction pour dresser un plan d'intervention en cas de cyberincident, et soutenir les efforts liés à la poursuite des activités qui sont déployés pour composer avec les cyberincidents et les atteintes à la protection des données;
- Veiller à ce que la société ait accès aux ressources du programme de cybersécurité qui peuvent assurer l'établissement, le maintien et la gouvernance du programme;
- Veiller à ce que la direction crée une culture de la sécurité suffisamment rigoureuse qui comprend la formation et la sensibilisation des employés.

3.2 PRINCIPAUX ÉLÉMENTS DU PROGRAMME DE CYBERSÉCURITÉ

La cybersécurité ne relève pas uniquement des technologies de l'information (TI). C'est plutôt un élément clé du succès de toute activité d'une entreprise. Cette question devrait être gérée de manière proactive par les dirigeants de la société, lesquels exercent les responsabilités suivantes :

Tenue d'un inventaire des actifs
Comprendre les actifs informationnels et les risques de la société en veillant à ce que les données critiques de la société, ses systèmes de TI et ses actifs soient inventoriés, et à ce que des mesures de sécurité appropriées soient prises en fonction de leur nature délicate. Un audit de confidentialité permet d'obtenir des détails sur les renseignements personnels que recueille et utilise la société. Un audit de système fournit une certaine assurance quant à l'accès aux systèmes critiques et aux contrôles en place.

Réalisation d'évaluations des risques
Les lois, les règlements et les obligations contractuelles standard en matière de sécurité des données sont souvent fondées sur la norme de la décision raisonnable pour l'évaluation des mesures de protection appliquées. Il est raisonnable, au sein du secteur des valeurs mobilières, d'effectuer des évaluations des risques de menace pour les systèmes critiques de la société. Une évaluation des risques de menace a pour but de définir et de prioriser les données et les systèmes critiques, de déceler les menaces qui planent sur les actifs informationnels de la société, de repérer les vulnérabilités potentielles et de comprendre les répercussions d'une intrusion sur la société.

Élaboration et maintien d'un programme écrit de sécurité de l'information
Un programme écrit établit les normes que doivent respecter les employés de la société, les sous-traitants et les principales personnes intéressées ainsi que les comportements qu'on attend d'eux. Un programme bien rédigé peut aider la société :

- à évaluer périodiquement les risques de manière proactive et à mettre en place des mesures de sécurité pour protéger les renseignements personnels et autres renseignements sensibles;
- à informer les employés et autres parties intéressées des mesures qu'ils doivent prendre;
- à communiquer au personnel et aux parties intéressées les attentes en matière de sécurité des données;
- établir les étapes prudentes et raisonnables que le personnel devrait suivre pour protéger les renseignements personnels et autres renseignements sensibles.

Élaboration et application d'une politique de sécurité de l'information
Le présent document établit les fondements d'un programme de sécurité de l'information efficace. Les politiques définissent les comportements qui sont attendus du personnel et des sous-traitants, et décrivent clairement les étapes que devraient suivre les personnes ayant

accès à l'information pour protéger les actifs informationnels de la société. En l'absence d'une politique de sécurité de l'information efficace et accessible, il est difficile pour une société de corriger les comportements qui vont à l'encontre des bonnes pratiques. Les sujets suivants sont notamment abordés dans une politique de sécurité de l'information :

- Attentes de la direction à l'égard du personnel et des sous-traitants;
- Catégories de données utilisées pour attribuer des niveaux de risque et de protection;
- Utilisations par le personnel des actifs informationnels de la société, y compris le contrôle de l'accès et les utilisations acceptables;
- Moyens employés par la société pour protéger et gérer ses actifs informationnels;
- Intervention en cas de cyberincident;
- Restriction des échanges avec les parties externes, notamment les fournisseurs et les clients;
- Programmes de gestion des risques et de conformité.

Formation et sensibilisation

Les employés et les sous-traitants sont parmi les meilleurs défenseurs de la sécurité de l'information d'une société, mais représentent aussi pour celle-ci la plus grande vulnérabilité. Les actes malveillants et, beaucoup plus souvent, les actes accidentels du personnel sont la plus grande cause des atteintes à la protection des données. Créer une culture de responsabilité partagée de la sécurité et offrir de la formation continue ciblée sur les façons d'éviter les cyberrisques sont les éléments de base d'un programme de sécurité efficace. La formation destinée aux employés devrait avoir les objectifs suivants :

- expliquer la politique de sécurité de la société, y compris les raisons sous-jacentes de la politique;
- communiquer aux employés leur obligation en matière de conformité et leur responsabilité personnelle à l'égard des actifs informationnels auxquels ils ont accès;
- fournir aux employés les ressources et le soutien spécialisé dont ils ont besoin pour éviter tout risque pour la sécurité;
- expliquer comment les employés doivent signaler les incidents de sécurité;
- offrir une formation plus détaillée aux employés qui ont accès à des systèmes et à des renseignements spécialisés présentant un plus grand risque pour la société.

Gestion des risques que présentent les fournisseurs

Pratiquement toutes les sociétés se fient à des tiers fournisseurs pour certains éléments clés de leurs processus opérationnels. De plus en plus, les entreprises sont forcées d'automatiser leurs processus et de sous-traiter certaines fonctions clés. Les cybercriminels se servent de tiers fournisseurs de services comme vecteurs d'attaque pour atteindre leur cible principale. Compte tenu des risques connus que posent les relations avec des tiers fournisseurs, le secteur s'attend normalement à ce que les sociétés exercent une surveillance diligente des fournisseurs et appliquent des mécanismes disciplinaires dans l'éventualité de manquements, d'atteintes à la protection des données ou d'incidents de sécurité importants.

Lorsqu'une société envisage d'avoir recours aux services d'un tiers fournisseur, elle devrait prendre les mesures suivantes :

- Effectuer un contrôle préalable pour déterminer si les contrôles de sécurité et de confidentialité d'un fournisseur potentiel sont comparables aux siens;
- Imposer à tous les fournisseurs des conditions contractuelles standard les obligeant à respecter ou à surpasser ses propres pratiques; demander au fournisseur de lui indiquer en quoi les normes de ce dernier sont différentes de ses propres pratiques si elle n'a pas le pouvoir de négociation nécessaire pour lui imposer ses propres normes;
- Assurer une surveillance continue et veiller à l'application des normes grâce à des privilèges contractuels en matière d'audit et à des paramètres de déclaration qui permettent d'effectuer une évaluation éclairée des risques pour la confidentialité et la sécurité des données. Lorsque la relation d'affaires prend fin, vérifier que les données lui sont retournées ou qu'elles sont raisonnablement détruites, et que la preuve de leur destruction est fournie.

3.3 ASSURANCE CONTRE LES CYBERRISQUES

Le marché de l'assurance continue d'évoluer en ce qui concerne les produits qui présentent des cyberrisques. Bien que les courtiers membres souscrivent une police d'assurance des institutions financières (PAIF) et une assurance responsabilité commerciale générale pour couvrir toute perte liée à leurs activités commerciales, la plupart des polices d'assurance de ce genre ne comprennent pas de protection contre les pertes résultant d'une atteinte à la protection des données ou d'autres cyberincidents. Les polices d'assurance contre les cyberrisques varient, et les sociétés devraient être conscientes des types de risques auxquels elles s'exposent et du type de protection contre ces risques.

Selon la police, la cyberassurance peut couvrir à la fois les coûts de première partie découlant d'un cyberincident ou d'une cyberinfraction et fournir une couverture-responsabilité contre le recours de tiers.

Coûts de première partie

Les coûts de première partie sont les coûts qu'une société engage lorsqu'elle enquête sur les effets d'une infraction ou d'un incident et prend des mesures pour atténuer ces effets et se conformer aux lois et règlements en matière de protection des renseignements personnels. Il arrive souvent que la société engage ces coûts même si elle ne fait pas l'objet d'une poursuite par un client ou un employé pour atteinte à la sécurité ou à la vie privée. Ces coûts sont notamment les suivants :

- Frais juridiques;
- Coûts des notifications en cas d'atteinte à la protection des données;

- Coûts des enquêtes judiciaires;
- Coûts de la surveillance du crédit ou de l'identité;
- Coûts du centre d'appels;
- Coûts des relations publiques;
- Coûts de l'interruption des activités.

Réclamations de tiers
La cyberassurance fournit également une couverture-responsabilité contre le recours de tiers et couvre les coûts suivants :

- Frais de défense;
- Coûts des règlements en faveur de tiers;
- Amendes assurables imposées par un organisme de réglementation à la suite d'une enquête ou d'une procédure réglementaire.

En plus d'offrir une protection contre toute perte financière éventuelle, une cyberassurance peut aider considérablement une société à améliorer son intervention en cas d'incident. Les compagnies d'assurances offrent aux titulaires de police un encadrement et des ressources dans l'éventualité d'un incident. Un « accompagnateur en gestion d'incident » est, dans la plupart des cas, un avocat qui agit à titre de conseiller de confiance indépendant pendant toute la durée de l'incident. L'accompagnateur en gestion d'incident maintient aussi un lien entre la société et d'autres tiers fournisseurs comme les enquêteurs judiciaires, afin de protéger la société en revendiquant des privilèges juridiques sur tout nouveau renseignement sensible.

Autre couverture d'assurance
Bien que les coûts mentionnés ci-dessus soient ceux qui sont habituellement engagés lors d'une atteinte à la protection des données, la cyberassurance ne couvre pas la gamme complète des autres coûts associés aux pertes potentielles liées à un cyberincident. Prenons l'exemple d'un système informatique qui est piraté dans le but de recueillir des renseignements servant à donner des instructions frauduleuses de transfert de fonds à des employés autorisés. Même si la pénétration du système informatique en vue de recueillir des données et de donner des instructions frauduleuses peut être couverte, la perte réelle découlant du transfert de fonds ne l'est pas[13].

En plus d'une protection de cyberassurance, les sociétés devraient également se demander si elles ont besoin d'une couverture-responsabilité pour leurs administrateurs et leurs dirigeants. Dans l'éventualité de pertes résultant d'un cyberincident, les membres du conseil et les dirigeants pourraient être tenus personnellement responsables. Par exemple, les parties intéressées comme les investisseurs et les clients pourraient engager des poursuites en alléguant que les membres du conseil et les dirigeants n'ont pas respecté leur obligation fiduciaire parce qu'ils n'ont pas assuré une gestion adéquate des cyberrisques. Une police

[13] La couverture pour de telles pertes peut être limitée dans le cas d'une police d'assurance des institutions financières (PAIF), selon les prorogations.

d'assurance pour les administrateurs et les dirigeants aiderait à couvrir les coûts associés à de telles poursuites.

Les assureurs prévoient différentes conditions et limitations dans leurs polices d'assurance. Les pertes pourraient être couvertes par différentes polices, selon les allégations et les pertes en cause. Les sociétés devraient examiner attentivement avec leur courtier d'assurance les scénarios de perte probables ainsi que le type de couverture dont elles ont besoin pour être suffisamment protégées.

3.4 PRINCIPAUX FACTEURS JURIDIQUES

Les dirigeants d'une société doivent non seulement être au courant des lois et des cadres réglementaires en matière de cybersécurité et de gestion des données sensibles, mais ils doivent aussi s'y conformer. Par exemple, en vertu de l'article 3703 des Règles de l'OCRCVM, les courtiers membres de l'OCRCVM sont tenus de signaler à l'organisme tout incident de cybersécurité[14]. Au Canada, les courtiers membres doivent respecter certaines autres lois pertinentes, notamment les suivantes :

- la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), telle que modifiée par la *Loi sur la protection des renseignements personnels numériques*, qui protège les renseignements personnels et s'applique aux organismes canadiens du secteur privé recueillant, utilisant ou communiquant des renseignements personnels dans le cadre de leurs activités commerciales;
- les lois provinciales en matière de protection des renseignements personnels du secteur privé qui pourraient s'appliquer aux courtiers membres exerçant dans ces provinces plutôt que la LPRPDE, si ces lois provinciales sont considérées comme similaires en grande partie à la LPRPDE[15];
- les lois et les règlements propres au secteur financier, notamment, selon les activités professionnelles du courtier membre, la *Loi sur les banques*, la *Loi sur les sociétés d'assurances* et les lignes directrices publiées par le Bureau du surintendant des institutions financières;
- d'autres lois et règlements conçus pour protéger les données, les actifs, les intérêts commerciaux, les secrets commerciaux et les contrats commerciaux à risque.

Les sociétés en activité dans des territoires à l'extérieur du Canada peuvent être visées par les lois et les règlements applicables de ces territoires relatifs à la protection de leurs données

[14] Les obligations de signalement prévues par la Règle de l'OCRCVM sont abordées dans l'Avis de l'OCRCVM 19-0194, et des indications supplémentaires sous forme de foire aux questions sont fournies dans l'Avis de l'OCRCVM 19-0195.

[15] Trois provinces ont édicté des lois en matière de protection des renseignements personnels pour le secteur privé qui sont considérées par le gouvernement du Canada comme similaires en grande partie à la LPRPDE – la Colombie-Britannique, l'Alberta et le Québec.

critiques et au signalement des événements importants qui pourraient avoir une incidence sur ces données. Au Canada, ailleurs que dans les provinces régies par les lois provinciales en matière de protection des renseignements personnels, la LPRPDE prévoit :

- des protections générales pour les renseignements personnels;
- les mesures que devraient prendre les sociétés pour protéger la communication par inadvertance de renseignements;
- les exigences relatives au signalement en temps opportun des infractions possibles.

La LPRPDE est appliquée par le Commissariat à la protection de la vie privée (CPVP). Elle exige que les sociétés mettent en place des procédures et nomment des responsables des interventions en cas d'atteinte à la protection des données et autres incidents liés aux renseignements personnels. Le CPVP pourrait considérer l'omission d'une société d'élaborer, de mettre en œuvre et de tenir à jour un plan d'intervention en cas de cyberincident comme un non-respect de la norme de la décision raisonnable de la LPRPDE en ce qui concerne les mesures de sécurité.

3.5 POLITIQUES ET PROCÉDURES

La politique de sécurité expose clairement les objectifs de la société. Elle établit non pas des lignes directrices, mais une conduite obligatoire.

L'expression « politique de sécurité » est utilisée en connaissance de cause plutôt que « politique de cybersécurité ». La sécurité englobe la sécurité physique, la sécurité du personnel, la cybersécurité, de même que le soutien des pratiques de poursuite des activités de l'entreprise. Bien que le présent guide porte plus précisément sur la cybersécurité, il est impossible d'appliquer un programme efficace de cybersécurité sans y intégrer les autres aspects de la sécurité.

La création d'une politique de sécurité exige que la direction consigne les contrôles qui sont nécessaires à la gestion des risques qu'elle est disposée à prendre. Les dirigeants d'une société devraient connaître les risques pour la sécurité avant d'élaborer une stratégie de cybersécurité éclairée.

Toute politique de sécurité de l'information devrait comprendre les éléments clés suivants :

- Tous les renseignements, les systèmes, les installations, les programmes, les réseaux de données et tous les utilisateurs de la technologie au sein de l'organisation (à l'interne et à l'externe), sans exception;
- Une méthode de classification de l'information bien définie ainsi que des définitions axées sur le contenu pour les catégories d'information, plutôt que des définitions plus générales de type « confidentiel » ou « restreint »;
- Les objectifs de la direction au chapitre de la manipulation sécurisée de l'information de chacune des catégories;

- La place de la politique dans le contexte des autres directives et documents de la direction;
- Des renvois aux documents connexes, notamment aux normes et lignes directrices du secteur;
- Des instructions précises sur les mandats de l'ensemble de l'organisation au chapitre de la sécurité (p. ex. aucune transmission des mots de passe);
- La désignation précise des rôles et responsabilités établis;
- Les conséquences de la non-conformité (p. ex. mesures pouvant aller jusqu'au congédiement ou à la résiliation du contrat)[16].

La mise en œuvre d'une politique ne constitue pas un événement unique; il s'agit plutôt d'un processus continu réexaminé au fil de l'évolution des modèles d'affaires, des relations et des technologies. En l'absence de politiques et de procédures, la gouvernance du programme de cybersécurité ne peut être efficace.

[16] CSO Online, *How to write an information security policy* (en anglais seulement).

4. CADRE OPÉRATIONNEL

Les dirigeants d'une société doivent avoir une façon d'évaluer l'état de préparation de leur société par rapport à celui des pairs et du secteur des valeurs mobilières dans son ensemble.

4.1 CADRE DE CYBERSÉCURITÉ DU NIST

Les cybermenaces exploitent la complexité et l'interdépendance croissantes des systèmes et des infrastructures essentielles, posant ainsi un risque pour la sécurité, l'économie et la santé publique d'une nation. Le National Institute of Standards and Technology (NIST) a été chargé de faciliter et de soutenir l'élaboration de cadres de gestion des cyberrisques pour renforcer la résilience des secteurs. Selon le cadre de cybersécurité du NIST (en anglais seulement) (le **cadre**), les organisations doivent utiliser des facteurs opérationnels pour orienter leurs activités de cybersécurité, et tenir compte des cyberrisques dans leurs processus de gestion des risques.

Le cadre permet aux organisations, quels que soient leur taille, le degré de risque pour la cybersécurité et la sophistication de leur programme de cybersécurité, d'appliquer les principes et les pratiques exemplaires de la gestion des risques pour améliorer leur sécurité et leur résilience.

Il s'applique aux organisations qui dépendent de la technologie, que leur objectif de cybersécurité soit essentiellement la TI, les systèmes de contrôle industriels, les systèmes cyberphysiques ou, plus généralement, les appareils connectés, y compris l'Internet des objets (IDO)[17]. Le cadre peut aider les organisations à aborder la cybersécurité selon ses répercussions sur la protection des renseignements personnels des clients, des employés et d'autres personnes.

Le cadre est constitué de trois parties.

- Cœur du cadre :
  Le cœur du cadre est un ensemble d'activités de cybersécurité, de résultats souhaités et de renvois informatifs qui sont communs à tous les secteurs et à toutes les infrastructures essentielles.

- Profils :
  Les profils aident les organisations à prioriser leurs activités de cybersécurité et à harmoniser ces activités avec les exigences de leur mission ou de leurs affaires, leur tolérance au risque et leurs ressources. Les éléments du cœur sont constitués de directives détaillées pour l'élaboration de profils organisationnels individuels.

[17] L'IDO peut être décrit comme le prolongement de l'Internet et d'autres connexions de réseau à différents capteurs et appareils — ou « objets » — permettant même aux objets les plus simples comme les ampoules, les verrous et les sorties d'air d'avoir des fonctions informatiques et analytiques de haut niveau.

- Niveaux de mise en œuvre (**niveaux**) :
  Les niveaux sont un mécanisme qu'utilisent les organisations pour voir et comprendre les caractéristiques de leur méthode de gestion des cyberrisques, ce qui les aide à prioriser et à atteindre leurs objectifs en matière de cybersécurité.

Le cadre de cybersécurité fournit une structure aux multiples approches en matière de cybersécurité qui sont utilisées actuellement, en rassemblant les normes, les lignes directrices et les pratiques sectorielles qui se sont révélées efficaces.

4.2 POURQUOI SE FIER AU NIST?

Les courtiers membres peuvent choisir parmi tout un éventail de cadres de cybercontrôle. La norme internationale de sécurité ISO 27001 et le référentiel COBIT sont également des cadres de contrôle bien établis. Ces normes peuvent être facilement mises en correspondance avec le cadre de cybersécurité du NIST.

Le cadre de cybersécurité du NIST a été choisi comme cadre directeur pour ce projet en raison de son langage commun et de sa méthode systématique de gestion des cyberrisques. Le cadre de cybersécurité du NIST est accessible aux dirigeants comme aux responsables des TI, ce qui favorise les communications de bout en bout sur la gestion des risques dans l'ensemble de l'organisation. Les organisations qui dépendent du NIST sont très variées. Il y a des hôpitaux, des institutions financières, des universités et des collèges ainsi que des organisations qui soutiennent les infrastructures essentielles. Les courtiers membres qui souhaitent en apprendre davantage sur les principes et les contrôles de sécurité individuels peuvent lire la multitude de publications accessibles sur Internet en plus de la présente publication.

4.3 APPROCHE PROGRESSIVE

Les risques seront toujours différents d'une organisation à une autre selon le type de menace, les vulnérabilités et la tolérance au risque. De même, la façon de mettre en œuvre les pratiques du cadre de cybersécurité du NIST sera différente d'une organisation à une autre. Cette latitude est importante compte tenu de la fluidité de l'environnement des cybermenaces et des moyens souvent restreints consacrés à la gestion de la cybersécurité.

Les courtiers membres devraient adopter une approche progressive pour la mise en œuvre des mesures de protection applicables, en fonction de l'évaluation de leurs capacités en matière de cybersécurité (c.-à-d. niveau 1, 2, 3 ou 4 du NIST), suivie d'une évaluation personnalisée des mesures de protection applicables aux sous-catégories de chacune des fonctions du NIST (c.-à-d. Déterminer, Protéger, Déceler, Intervenir et Reprendre les activités), selon les capacités évaluées.

Autrement dit, l'évaluation peut servir à prioriser les dépenses de manière à maximiser l'effet des sommes dépensées en fonction de la capacité d'un courtier membre à mettre en œuvre des mesures de protection applicables.

Il est important de préciser que les niveaux ne représentent pas le degré de maturité des organisations. Ils visent plutôt à aider les organisations à prendre des décisions quant à la façon de gérer les cyberrisques et aux aspects qu'elles devraient traiter en priorité et auxquels elles pourraient affecter des ressources supplémentaires. La progression vers les niveaux supérieurs est recommandée dans les cas où une analyse coûts-avantages indique qu'il est possible de réduire les cyberrisques de manière efficace.

4.4 ÉVALUATION DES COÛTS, DES DIFFICULTÉS ET DE L'ÉCHÉANCIER

Les organisations devraient déterminer et prioriser des améliorations faisables et rentables à court, à moyen et à long terme après avoir examiné leurs exigences opérationnelles et les risques importants, et après avoir pris des décisions raisonnables et éclairées sur le plan de la cybersécurité à l'aide de leurs évaluations. Il s'agira d'évaluer approximativement les coûts, les difficultés et l'échéancier pour chaque mesure de protection sélectionnée, en fonction du niveau du NIST.

4.5 DESCRIPTION DES PROFILS

Une organisation de **niveau 1** est définie comme suit :

- Les pratiques de gestion des cyberrisques de l'organisation n'ont pas été officialisées;
- Le risque est géré de manière ponctuelle et parfois de manière réactive;
- La priorisation des activités de cybersécurité n'est peut-être pas directement fondée sur les objectifs liés aux risques de l'organisation, les menaces ou les exigences liées à la mission ou aux activités de l'organisation;

- Le personnel de l'organisation est peu sensibilisé aux cyberrisques, et aucune méthode de gestion de ces risques n'a été établie à l'échelle de l'organisation;
- L'organisation gère les cyberrisques de manière irrégulière, au cas par cas, selon les divers renseignements acquis auprès de sources externes;
- L'organisation ne dispose peut-être pas de processus qui permettent l'échange de renseignements sur la cybersécurité au sein de l'organisation;
- L'organisation n'a peut-être pas établi de processus visant à favoriser la participation à la coordination, ou la collaboration avec d'autres entités.

Une organisation de **niveau 2** est définie comme suit :

- Les pratiques de gestion des risques sont approuvées par la direction, mais ne figurent pas dans la politique organisationnelle;
- La priorisation des activités de cybersécurité et des besoins de protection est directement fondée sur les objectifs en matière de risque de l'organisation, les menaces ou les exigences liées à la mission ou aux activités de l'organisation;
- Le personnel de l'organisation est sensibilisé aux cyberrisques, mais aucune méthode de gestion de ces risques n'a été établie à l'échelle de l'organisation;
- Les renseignements sur la cybersécurité sont transmis au sein de l'organisation de manière informelle;
- Les programmes et les objectifs de l'organisation en matière de cybersécurité sont pris en considération par certains échelons de l'organisation, mais pas tous;
- Une évaluation des cyberrisques associés aux actifs externes et internes de l'organisation est effectuée, mais elle n'est habituellement pas réitérée;
- De manière générale, l'organisation comprend son rôle au sein de l'écosystème élargi en ce qui concerne ses propres dépendances et celles d'autres parties, mais pas les deux;
- L'organisation collabore avec d'autres entités et reçoit des renseignements d'autres entités en plus de générer certains de ses propres renseignements, mais ne transmet peut-être pas de renseignements aux autres;
- L'organisation connaît les cyberrisques associés à la chaîne d'approvisionnement qui englobe les produits et services qu'elle offre et utilise, mais n'a pas pris de mesures cohérentes ou officielles par rapport à ces risques.

Une organisation de **niveau 3** est définie comme suit :

- Les pratiques de gestion des risques de l'organisation sont approuvées officiellement et énoncées dans une politique;
- Les pratiques de cybersécurité de l'organisation sont périodiquement mises à jour en fonction de l'application des processus de gestion des risques aux changements qui sont apportés aux exigences liées à la mission et aux activités de l'organisation, et en fonction de l'évolution des cybermenaces et des technologies;
- L'organisation a adopté une méthode globale de gestion des cyberrisques;
- Les politiques, les processus et les procédures axés sur les risques sont définis, mis en place comme prévu et révisés;

- Les méthodes cohérentes en place permettent de faire face efficacement aux risques qui évoluent;
- Le personnel possède les connaissances et les compétences nécessaires pour exercer leurs fonctions et leurs responsabilités;
- L'organisation connaît ses dépendances et ses partenaires, et reçoit de ceux-ci des renseignements qui favorisent la collaboration au sein de l'organisation et la prise de décisions de gestion fondées sur les risques dans le cas d'un événement.

Une organisation de **niveau 4** est définie comme suit :

- L'organisation adapte ses pratiques de cybersécurité selon les leçons apprises et les indicateurs de prédiction découlant des activités de cybersécurité précédentes et actuelles;
- Grâce à un processus d'amélioration continue qui intègre des technologies et des pratiques de cybersécurité de pointe, l'organisation s'adapte activement à l'environnement changeant des cybermenaces et réagit rapidement aux menaces sophistiquées et changeantes;
- Une méthode de gestion des cyberrisques a été établie à l'échelle de l'organisation; elle est constituée de politiques, de procédures et de processus fondés sur les risques qui permettent à l'organisation de réagir aux éventuels incidents de cybersécurité;
- La gestion des cyberrisques fait partie de la culture de l'organisation, et elle évolue en fonction de la connaissance des activités précédentes, des renseignements communiqués par d'autres sources et des activités sur les systèmes et les réseaux;
- L'organisation gère les risques et échange activement des renseignements avec ses partenaires pour que les renseignements qui sont transmis soient exacts et à jour, et ce, dans le but d'améliorer la cybersécurité avant que des incidents de cybersécurité ne surviennent.

5. DIRECTIVES POUR LA MISE EN ŒUVRE D'UN PROGRAMME OPÉRATIONNEL

La section 3 décrit les obligations qu'ont les sociétés en matière de cybersécurité. La section 4 présente le concept des niveaux de sécurité et précise que les améliorations structurées du programme de cybersécurité peuvent collectivement faire passer une société d'un niveau à un autre. La présente section énonce les étapes que la société doit suivre à chaque niveau pour mettre en place un programme de sécurité efficace. La section suivante traite des pratiques exemplaires recommandées pour un programme de sécurité efficace.

La prise de décisions et les communications font partie intégrante de la gouvernance opérationnelle. Celle-ci permet de s'assurer que des responsabilités claires sont assignées en matière de communications, de processus et d'actifs. Des politiques, des normes, des mesures et des contrôles adaptés sont élaborés pour que les employés et les fournisseurs puissent comprendre et exécuter leurs rôles et responsabilités, et pour indiquer clairement les types de comportements qui sont attendus et les comportements qui sont inacceptables. Enfin, un examen délibéré du programme et des évaluations de la conformité fournit des renseignements sur l'efficacité des responsabilités, des politiques de communication, des contrôles et du programme de gouvernance proprement dit.

Essentiellement, la gouvernance opérationnelle fait en sorte que le plan de sécurité visant à protéger les actifs les plus précieux d'une société soit en place et tenu à jour. Le processus de détermination des éléments clés d'un tel plan est décrit dans le graphique ci-dessous.

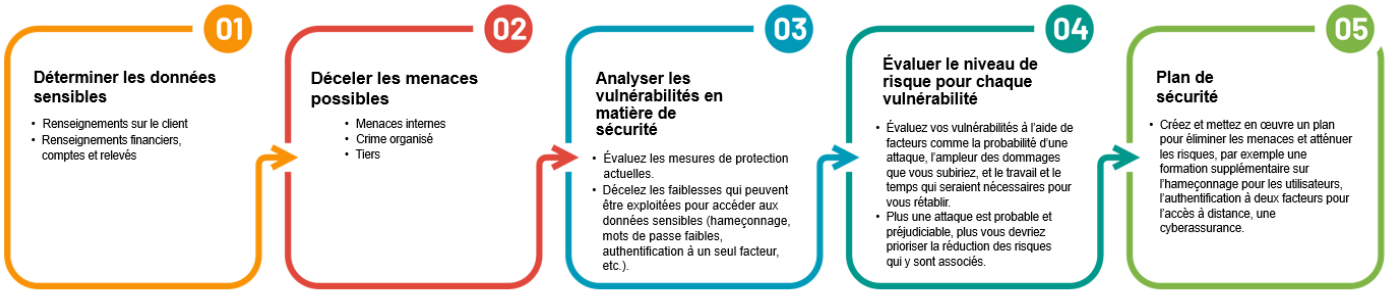


Figure 1 : Plan de sécurité opérationnelle

Pour créer un plan qui assurera la sécurité des actifs de votre société, vous devez vous concentrer sur les **trois objectifs fondamentaux** suivants[18] :

- **Confidentialité**
  Tous les renseignements importants en votre possession doivent être tenus confidentiels. L'accès à ces renseignements doit se limiter aux personnes (ou systèmes) qui ont l'autorisation de les consulter.

[18] Guide Pensez cybersécurité pour les petites et moyennes entreprises

- **Intégrité**
  Maintenir l'intégrité des renseignements pour qu'ils demeurent complets, intacts et non corrompus.
- **Accessibilité**
  Garantir l'accessibilité des systèmes, des services et des renseignements au moment où l'organisation ou ses clients en ont besoin.

Grâce à un plan et à des objectifs clés, une société pourra prendre des mesures de protection qui permettront d'exercer les principales fonctions du cadre de cybersécurité décrites ci-après[19] :

1. Protéger les actifs à l'aide de mesures de protection appropriées;
2. Déceler les intrusions, les infractions à la sécurité et les accès non autorisés;
3. Intervenir dans l'éventualité d'un incident de cybersécurité;
4. Se remettre d'un incident de cybersécurité en rétablissant les activités et services habituels.

5.1 DILIGENCE RAISONNABLE ET DEVOIR DE DILIGENCE

La création et la mise en œuvre d'un plan de sécurité aideront toute société à faire preuve de diligence raisonnable pour protéger ses actifs de valeur et respecter les exigences juridiques inhérentes aux lois sur la protection des renseignements personnels.

Grâce à la cybergouvernance opérationnelle, la prise de décisions et les communications sont axées sur le bon fonctionnement au quotidien des protections et des contrôles dont dépend l'organisation (le plan de sécurité).

Une bonne cybergouvernance se compose d'éléments qui peuvent être examinés et auxquels on peut se fier, notamment les suivants :

- **politiques** : des documents qui énoncent l'intention de la direction de fournir des lignes directrices sur lesquelles sont fondées les décisions. La politique et le plan d'intervention en cas d'incident d'une société en sont des exemples, la sensibilisation à la sécurité en est un autre exemple;
- **mesures d'efficacité** : elles permettent de comprendre et de contrôler les processus de cybersécurité. Les vulnérabilités non corrigées constituent un exemple;
- **conformité :** les documents requis pour soutenir le caractère vérifiable des processus et des décisions.

À mesure que les capacités s'améliorent, les efforts et les investissements sont de plus en plus axés sur les bonnes pratiques de cybersécurité et le devoir de diligence de la société. La gouvernance opérationnelle garantit qu'une norme de diligence raisonnable est appliquée pour protéger les actifs et les renseignements de la société. Les responsabilités qu'assument les

[19] National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity*, 2014.

dirigeants pour d'autres aspects de l'entreprise s'appliquent aussi à la cybersécurité, par exemple la responsabilité de veiller à ce que les processus et les résultats soient vérifiables. Les **documents clés** comprennent entre autres les inventaires des actifs et des services, les examens effectués par des tiers, les évaluations des risques et les politiques de gestion des risques. Ces documents, une fois qu'ils ont été élaborés et officialisés, doivent être revus et mis à jour périodiquement, et permettre de vérifier que la société fait preuve de diligence raisonnable sur une base constante et régulière.

5.2 ÉTAT DE PRÉPARATION

Un aspect clé de la diligence raisonnable est l'état de préparation et la résilience. Les investissements qu'une société fait dans un plan de sécurité et de cybersécurité réduisent la probabilité d'un cyberincident et des conséquences qui en découlent, mais ils ne peuvent éliminer la probabilité qu'un cyberincident survienne. Les sociétés doivent se préparer, planifier et tester leurs capacités à intervenir et à reprendre leurs activités en cas de cyberincident important ou d'interruption de leurs activités.

La mesure dans laquelle une société est capable d'intervenir et de reprendre ses activités après un incident est directement liée à son état de préparation. L'état de préparation des fonctions de TI et de cybersécurité peut être un aspect clé d'une intervention en cas d'incident. Les communications et les capacités juridiques et de leadership sont tout aussi importantes, et bien souvent plus importantes, particulièrement lors d'interventions faisant suite à une atteinte potentielle à la sécurité des renseignements personnels et financiers.

Intervention en cas d'incident
Un plan d'intervention en cas d'incident bien rédigé et bien compris constitue un élément essentiel de la préparation. Les éléments d'un tel plan et la façon d'optimiser son utilisation sont décrits à la section 6.15.

Copies de sauvegarde
Les copies de sauvegarde des données et des renseignements clés sont l'un des éléments principaux de tout plan de résilience et de reprise adéquat. Les copies de sauvegarde des données permettent à l'entreprise de poursuivre ses activités sans trop d'interruption, selon les circonstances. Les copies de sauvegarde peuvent être particulièrement utiles lorsque l'entreprise a été victime d'un rançongiciel ou d'une attaque de virus ciblant le lecteur de disque dur. Il est essentiel que les copies de sauvegarde soient vérifiées périodiquement, protégées adéquatement et facilement accessibles, au besoin. Il est également recommandé qu'au moins une copie de sauvegarde soit gardée à l'externe.

Cyberexercices de simulation
Un cyberexercice de simulation est une activité de préparation à un incident ou à un sinistre qui permet aux participants de gérer un scénario de catastrophe simulé. Basé sur la discussion, l'exercice de simulation non seulement aide les participants à se familiariser avec le processus d'intervention, mais favorise aussi le leadership dont il faut faire preuve pour évaluer l'efficacité

des capacités d'intervention en cas d'urgence ou d'incident. Les employés clés présents lors de l'exercice ont l'occasion non seulement de se familiariser avec leur propre rôle dans des scénarios de catastrophe, mais aussi de voir comment l'intervention dans son ensemble se déroulera au sein de l'organisation.

Les exercices de simulation sont effectués en accéléré et permettent de passer en revue tous les aspects d'un scénario hypothétique, du début de l'incident aux activités menées après l'incident. Voici ce qui est évalué :

- les ressources internes;
- toute ressource externe appelée en renfort, par exemple un avocat, un accompagnateur en gestion d'incident ou une compagnie de cyberassurance;
- les communications qui seront transmises, les destinataires de ces communications et les moyens de communication.

Les scénarios d'exercice devraient permettre de tester les progrès de la société quant à son état de préparation aux cyberincidents et quant aux plans qui ont été élaborés pour gérer les scénarios probables. L'un des aspects essentiels de l'évaluation des conséquences potentielles d'un incident consiste à déterminer si les organismes de réglementation doivent être informés. Cela est particulièrement important dans le cas d'atteintes potentielles à la sécurité des renseignements personnels ou financiers.

Les résultats d'un exercice de simulation devraient fournir des renseignements utiles pour les interventions futures en cas d'incident et la planification de la reprise après sinistre, et ils devraient indiquer les nouvelles lignes directrices et pratiques que l'organisation pourrait devoir mettre en place. L'exercice peut révéler des lacunes dans les connaissances du personnel ou des défauts de sécurité qui doivent être corrigés. Normalement, les exercices permettent de confirmer que, même si l'intervention des TI et de la sécurité et les capacités de rétablissement sont importantes, les communications transmises par l'entreprise et les décisions prises par cette dernière, particulièrement durant l'incident, sont essentielles pour déterminer le succès d'une intervention en cas d'incident.

Les exercices de simulation devraient être effectués régulièrement, soit de trois à quatre fois par année. Il est possible d'élaborer des scénarios à partir des événements récents qui sont survenus dans le secteur. Un exercice peut durer de 45 minutes à 2 heures, selon la complexité de l'incident et le nombre de participants.

À la suite de l'exercice, les participants et les animateurs peuvent rédiger un rapport qui donne des détails sur les principales constatations ou questions soulevées durant l'exercice.

Planification de la poursuite des activités

Un plan de poursuite des activités (PPA) est un document qui décrit comment une entreprise poursuivra ses activités lors d'une interruption de service imprévue. Ce plan est plus exhaustif qu'un plan de reprise après sinistre, qui est axé strictement sur le rétablissement des capacités de TI. Un PPA décrit les mesures qui doivent être prises pour assurer le maintien des processus

de l'entreprise. Il énonce les dépenses accidentelles et, dans certains cas, les solutions de rechange, les processus, les actifs, les ressources humaines et les partenaires d'affaires. Par définition, le PPA couvre tous les aspects de l'entreprise qui peuvent être touchés. Les principales interruptions qui devraient être planifiées sont les suivantes :

- la perte des bureaux pendant une durée prolongée;
- l'incapacité d'accéder aux bureaux pendant plus d'une semaine;
- une pandémie ou une crise de santé publique;
- la perte d'employés clés;
- un cyberincident.

Le plan peut prévoir des stratégies détaillées de maintien des activités de l'entreprise en cas de pannes de courte durée et de longue durée. Il comporte habituellement une liste de vérification qui indique les fournitures et le matériel, l'emplacement d'autres lieux de travail et les protocoles pour le travail à distance. Le plan désigne également les administrateurs du plan et fournit les coordonnées des employés clés, des fournisseurs des centres de secours et des intervenants d'urgence.

Il est important de noter que, aux termes des articles 4710 à 4714 des Règles de l'OCRCVM, tous les courtiers membres doivent avoir un PPA à jour et le mettre à l'essai annuellement.

5.3 ÉVALUATION DES MENACES ET DES VULNÉRABILITÉS[20]

Les cybercriminels continuent de tirer profit des vulnérabilités de base des systèmes informatiques, notamment des fonctionnalités non corrigées des systèmes d'exploitation, des mots de passe faibles et des connaissances insuffisantes des utilisateurs finaux. Les organisations qui n'effectuent pas d'analyse des vulnérabilités et qui ne corrigent pas efficacement les faiblesses de leurs systèmes d'information risquent davantage que leurs systèmes informatiques soient compromis. Pour protéger leurs actifs informationnels contre la menace grandissante des cyberattaques qui ciblent les vulnérabilités des systèmes, un plus grand nombre d'organisations incluent des évaluations des vulnérabilités dans leurs programmes de cybersécurité. Ces évaluations permettent de déceler les vulnérabilités des systèmes informatiques. Les résultats de ces évaluations aident les organisations à localiser les cyberrisques[i]. Voici des recommandations en ce qui concerne l'évaluation des menaces et des vulnérabilités :

- utiliser périodiquement un outil automatisé pour évaluer les vulnérabilités de tous les systèmes du réseau; remettre des listes des priorités renfermant les vulnérabilités les plus importantes à chaque administrateur de système;
- s'abonner à un service de renseignement sur les vulnérabilités afin de demeurer au fait des nouvelles menaces et expositions au risque;

[20] Voilà un exemple de la façon dont les recommandations formulées dans le document de pratiques exemplaires seront comparées aux contrôles du cadre de cybersécurité du NIST.

- veiller à ce que les outils d'évaluation des vulnérabilités utilisés soient périodiquement mis à jour et renferment les renseignements sur les vulnérabilités les plus à jour possible;
- veiller à ce que les logiciels/applications informatiques soient mis à jour périodiquement à l'aide de correctifs de sécurité;
- soumettre les correctifs essentiels à des essais avant de les intégrer dans les systèmes de production.

5.4 ÉLABORATION D'UN PROGRAMME COMPLET

Lorsqu'elles élaborent le cadre de politique et les éléments de programme nécessaires, les sociétés devraient orienter leur réflexion vers les systèmes plutôt que d'envisager des solutions ou des contrôles de sécurité ponctuels. L'organisation fait preuve de diligence raisonnable lorsqu'elle examine les menaces et les vulnérabilités probables d'une façon systémique. Les fournisseurs externes peuvent certes aider à décrire l'environnement des menaces, mais ce sont les gens à l'interne qui connaissent les activités de l'organisation et les actifs informationnels et qui peuvent déterminer quelles sont les menaces générales qui planent sur leur société.

Une préparation efficace suppose non seulement d'adopter des contrôles de sécurité, mais également de planifier et de tester des scénarios de menace probables pour que les plans établis permettent à la société d'affronter toute interruption potentielle de ses activités.

6. RECOMMANDATIONS DE PRATIQUES EXEMPLAIRES

La cybersécurité est une responsabilité partagée – les personnes, les processus, les outils, les mesures de protection et les technologies contribuent tous à la protection des actifs d'une organisation. Les mesures de protection suivantes devraient être prises en compte lors de la conception d'un plan de cybersécurité. La mise en œuvre de mesures de protection qui sont conformes à l'appétit pour le risque d'une société permettra de concevoir et d'établir un plan qui répondra le mieux aux exigences et aux besoins opérationnels uniques de l'organisation.

Ce plan peut aussi être utile pour démontrer le devoir de diligence de la direction, et pour rassurer les tiers et les organismes de réglementation, au besoin.

6.1 ENQUÊTE DE SÉCURITÉ SUR LE PERSONNEL ET MENACES INTERNES

Habituellement, les organisations se concentrent principalement sur les menaces externes et appliquent des solutions techniques, notamment l'installation de programmes antivirus pour protéger leurs systèmes informatiques contre les logiciels malveillants, ou des pare-feu pour se protéger contre les menaces liées à Internet.

Des données publiées par McKinsey & Company en 2018 indiquent que 50 % des cyberinfractions étaient associées à une menace interne. De ce nombre, près de 40 % étaient associées à des employés malveillants – à peu près 44 % étaient le résultat soit de la négligence, soit de la contribution innocente d'une partie externe associée à un employé. Cela suppose que la cybersécurité des courtiers membres doit être axée également sur l'élément humain, particulièrement sur les candidats qui sont recrutés et sur la façon dont le comportement des employés change[21].

Voici certains risques que posent les menaces internes dans le secteur financier[22] :

- La divulgation non souhaitée de données confidentielles sur les clients et les comptes;
- La fraude et les pertes pécuniaires;
- La perte de propriété intellectuelle;
- La désorganisation des infrastructures essentielles;
- Des répercussions sur le plan réglementaire;
- La déstabilisation, la perturbation et la destruction de l'information, des applications, des contrôles et des protections de cybersécurité des institutions financières;
- L'embarras, les problèmes de relations publiques et l'atteinte à la réputation.

Selon le CERT Insider Threat Center de la Carnegie Mellon University[23], les employés qui posent le plus grand risque de menace interne sont :

[21] McKinsey & Company. *The Human Element of Cyber Risk* (en anglais seulement), 2018.
[22] Bunn, C. *A Focus on Insider Threats in Banking & Financial Institutions* (en anglais seulement), 2013.
[23] Ibid, p. 1.

- les employés mécontents qui estiment qu'on a manqué de respect à leur égard, et qui souhaitent se venger;
- les employés à la recherche d'un bénéfice qui croient pouvoir faire plus d'argent en vendant la propriété intellectuelle volée;
- les employés qui passent chez un concurrent ou qui démarrent une entreprise et qui, par exemple, volent des listes de clients ou des plans d'affaires pour se donner un avantage sur les concurrents;
- les employés qui se croient les propriétaires de la propriété intellectuelle qu'ils ont contribué à mettre au point et qui la prennent avec eux lorsqu'ils quittent l'organisation.

Les recommandations suivantes sont des recommandations utiles pour gérer les menaces internes[24].

- **Mettre sur pied une équipe pluridisciplinaire**
  Dans la mesure du possible, les organisations devraient avoir une équipe composée de professionnels des ressources humaines, de la sécurité et des services juridiques qui sont chargés de créer des politiques, de diriger la formation et de surveiller les employés à risque.
- **Comprendre les enjeux organisationnels**
  Les organisations doivent évaluer si elles s'exposent à un plus grand risque en raison de certains facteurs inhérents. Par exemple, les bureaux à distance, les fournisseurs et sous-traitants ainsi que les différences culturelles, politiques ou linguistiques pourraient engendrer des conflits.
- **Examiner les processus de vérifications préalables à l'emploi**
  Les renseignements recueillis au cours de ce processus aideront les gestionnaires chargés de l'embauche à prendre des décisions éclairées et à atténuer le risque d'embaucher un employé « à problèmes ».
- **Élaborer des politiques et des pratiques**
  Il s'agit d'une liste de contrôle des questions particulières liées aux politiques et aux pratiques qui doivent faire partie intégrante des structures de gouvernance de base d'une organisation.
- **Donner de la formation et des renseignements**
  Ces activités sont essentielles à l'efficacité des politiques, car les politiques et les pratiques qui ne sont pas reconnues, comprises et respectées peuvent avoir une efficacité limitée.
- **Surveiller les comportements douteux ou perturbateurs dès le processus d'embauche, et intervenir**
  Il est important de reconnaître que la diligence ne peut se limiter au processus d'embauche. Certains employés composent souvent difficilement avec des facteurs de stress externes, et cette situation peut nuire à leur rendement au travail.
- **Prévoir et gérer les situations défavorables dans le milieu de travail**

[24] Shaw, E.D. et Harley V. Stock, Ph. D. *Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property: Misreading the Writing on the Wall* (en anglais seulement), 2011.

Le fait pour les dirigeants de demeurer attentifs aux changements de comportement dans le milieu de travail et d'être prêts à venir en aide à l'employé à risque s'est révélé une stratégie efficace contre une menace interne naissante.

- **Exiger la séparation des tâches et restreindre l'accès**
  La séparation des tâches clés et la restriction de l'accès peuvent aussi contribuer à restreindre les occasions pour un employé de causer un préjudice à l'organisation. S'assurer périodiquement que les autorisations et les accès sont conformes à une politique de droit d'accès minimal afin de respecter les exigences opérationnelles soutient l'objectif global qui consiste à limiter le risque potentiel d'une menace interne.

Les courtiers membres peuvent atténuer les dommages susceptibles de découler des menaces internes en reconnaissant les torts que peuvent causer les employés en poste ou les employés qui ont quitté l'organisation.

Étude de cas (2018) : Recherches non autorisées dans des bases de données de la police[25]
Une employée civile temporaire, Erin Maranan, avait accès à de l'information classifiée par la police comme de l'information à diffusion très restreinte. Elle a effectué des dizaines de recherches illégales dans des bases de données de la police sur une période de 16 mois entre 2014 et 2015. Ses recherches lui ont donné accès à un catalogue de personnes dans les bases de données de la police, catalogue qui comprenait des photos, des descriptions physiques, des adresses, le nom de personnes connues ayant des liens avec la police et plus encore. M^me^ Maranan pouvait aussi voir les liens qui existaient entre ces personnes et les enquêtes criminelles. Certaines recherches qu'elle a effectuées visaient à recueillir de l'information sur des membres rivaux d'organisations criminelles, tandis que d'autres étaient soi-disant de simples recherches sur les membres d'un gang pour savoir quelle information la police détenait sur eux. Même si trois des personnes visées par les recherches de M^me^ Maranan ont été tuées plus tard, la Couronne n'a pu établir que M^me^ Maranan savait comment l'information serait utilisée, et il n'a pas été prouvé que la divulgation des renseignements a compromis les enquêtes en cours ou causé un préjudice à une personne en particulier.

M^me^ Maranan a été condamnée à un an de prison et à trois ans de probation après avoir plaidé coupable à une inculpation d'abus de confiance. Les relevés téléphoniques de M^me^ Maranan ont révélé qu'elle entretenait une relation personnelle avec un membre de gang présumé, sur qui elle aurait effectué des recherches à 17 occasions. Les renseignements auxquels M^me^ Maranan avait accès faisaient l'objet d'une telle restriction que même les personnes qui enquêtaient sur elle n'avaient pas les droits d'accès nécessaires pour les consulter.

6.2 SÉCURITÉ PHYSIQUE ET ENVIRONNEMENTALE

La sécurité physique des actifs constitue une première ligne de défense en cybersécurité. Le vol d'un ordinateur portable ou d'un téléphone intelligent peut avoir un effet très perturbateur sur

[25] The Toronto Star. *Civilian Toronto police employee jailed after conducting illegal database searches* (en anglais seulement), juin 2018.

une organisation. Les mesures de protection, tels les mots de passe et les NIP, doivent être accompagnées d'autres mesures de sécurité, comme des verrous qui empêchent le vol d'ordinateurs portables ou l'utilisation d'un système d'alimentation sans coupure afin de protéger le système d'information lors d'une panne de courant.

La sécurité physique englobe des mécanismes de défense contre les menaces suivantes :

Menaces humaines
Dommages causés par des personnes, par exemple un intrus qui pénètre dans une zone à accès restreint, ou une erreur commise par un employé;

Menaces environnementales
Dommages causés par les conditions climatiques, notamment la pluie, un incendie, une inondation;

Menaces pour les systèmes d'alimentation
Dommages causés par une interruption de l'approvisionnement énergétique qui peut nuire à un système d'information.

Les recommandations suivantes sont des recommandations en matière de sécurité physique et environnementale :

- Les employés devraient appliquer le principe du « bureau propre », c'est-à-dire qu'ils devraient ranger les documents renfermant des renseignements de nature délicate avant de quitter leur poste de travail. Un bureau propre évite que les renseignements de nature délicate ne se retrouvent entre les mains de personnes qui n'ont pas de raison légitime de les consulter, par exemple le personnel d'entretien et les gardiens de sécurité;
- Un employé devrait avoir accès à une aire de travail seulement s'il a une raison professionnelle légitime qui le justifie;
- Des procédures de gestion des visiteurs devraient être établies et faire en sorte que les visiteurs signent un registre à leur arrivée et à leur départ, et qu'ils soient accompagnés en tout temps lorsqu'ils sont dans les bureaux;
- L'utilisateur devrait restreindre l'accès au contenu de son ordinateur en verrouillant l'écran lorsqu'il s'absente de son poste de travail;
- Il est recommandé de protéger le système d'information contre les variations de l'alimentation électrique ou les pannes de courant, et de veiller à ce qu'il soit branché à un système d'alimentation sans coupure;
- Il est préférable d'effectuer périodiquement des copies de sauvegarde des renseignements pour être à l'abri des sinistres.

6.3 SENSIBILISATION À LA CYBERSÉCURITÉ ET FORMATION

Le risque d'une cyberattaque contre des institutions financières ne cesse de croître, à mesure que notre monde très branché crée des débouchés pour les cybercriminels. Étant donné que les institutions financières s'en remettent à des outils en ligne pour mieux communiquer avec les parties intéressées, elles demeurent la cible de cybercriminels souhaitant voler leur propriété

intellectuelle et leurs renseignements confidentiels. Le sondage *Global State of Information Security® Survey*, mené en 2018 par Price Waterhouse Coopers, révèle que les pertes financières moyennes attribuables aux incidents de cybersécurité qui sont déclarées par les entreprises dotées d'un programme de sensibilisation à la sécurité sont substantiellement moins élevées[26]. Il révèle par ailleurs qu'un programme efficace de sensibilisation à la sécurité exige des fonds suffisants.

Bon nombre d'organisations investissent massivement dans les contrôles techniques pour protéger leurs systèmes informatiques et leurs données. Cependant, les employés et les personnes à l'interne qui ne sont pas vigilants augmentent grandement les cyberrisques que court l'organisation lorsqu'ils ouvrent des courriels douteux ou ne protègent pas les renseignements de nature délicate stockés sur leur ordinateur ou transmis à partir de leur ordinateur. Le sondage *Cyberthreat Defense Report Survey* de 2019 révèle que la faible sensibilisation à la sécurité des employés demeure le plus important facteur nuisant à une défense efficace contre les cybermenaces[27].

Les recommandations suivantes sont des recommandations en matière de sensibilisation à la cybersécurité et de formation :

- Mettre en œuvre des politiques portant sur l'utilisation sûre et acceptable des systèmes informatiques;
- Rendre obligatoires la sensibilisation à la cybersécurité et la formation en cybersécurité pour tout le personnel. La formation peut se dérouler en classe, en ligne ou par séance vidéo, et elle devrait être offerte sur une base annuelle. Les attaques par piratage (p. ex. l'hameçonnage par courriel) visent souvent les cadres supérieurs; il est donc important que ces personnes suivent également la formation en cybersécurité;
- Veiller à ce que tous les membres du personnel comprennent :
    - leurs rôles et responsabilités en matière de cybersécurité;
    - que des sanctions seront imposées aux employés qui ne se conforment pas aux principes de sensibilisation à la cybersécurité et aux politiques de sécurité;
- Demander aux employés :
    - de ne pas ouvrir les courriels douteux ni de cliquer sur les liens suspects, quelle qu'en soit la source; de confirmer auprès de leurs collègues ou des hauts dirigeants les « demandes » inhabituelles ou suspectes, particulièrement si celles-ci concernent le transfert de fonds, l'achat de cartes-cadeaux, l'accès à de l'information à diffusion restreinte, etc.;
    - de ne pas connecter d'appareils au réseau, à moins d'avoir une raison professionnelle légitime de le faire ou d'utiliser des appareils approuvés;
    - d'appliquer de saines pratiques en matière de mot de passe;
    - d'être conscients des dangers et des usages sûrs des supports externes (clés USB et DC);

[26] Price Waterhouse Coopers. *Global State of Information Security Survey* (en anglais seulement), 2018.
[27] CyberEdge Group LLC. *Cyber Threat Defense Report* (en anglais seulement), 2019.

- Offrir de la formation continue et transmettre les connaissances obligatoires au moyen de séances vidéos ou de webinaires.

Étude de cas (2017) : Un Canadien accusé de louer ses services de pirate informatique international[28]

Des agents du renseignement russes ont demandé à des pirates informatiques criminels, dont le Canadien Karim Baratov, d'accéder sans y être autorisés aux ordinateurs de sociétés offrant des services Internet et de messagerie Web (Yahoo, Google, etc.), de maintenir l'accès non autorisé à ces ordinateurs et de voler des renseignements stockés dans ces ordinateurs.

Les victimes désignées de M. Baratov étaient des représentants du gouvernement russe, notamment de hauts dirigeants politiques et leurs conseillers, un responsable de l'application de la loi et un important banquier kazakh. M. Baratov et ses cocomploteurs ont adopté cette conduite aux fins de bénéfices commerciaux et de gains financiers personnels. M. Baratov employait des messages de « harponnage » conçus pour amener par la ruse des destinataires inconscients à donner accès à leur ordinateur et à leur compte.

6.5 SÉCURITÉ DU RÉSEAU

La connexion permanente d'une organisation à Internet l'expose à un milieu hostile de menaces externes et internes qui évoluent de façon très rapide.

La sécurité d'un réseau s'entend d'une activité visant à protéger la confidentialité, l'intégrité et l'accessibilité du réseau et des actifs informationnels sur lesquels il repose. De façon générale, la sécurité du réseau comporte trois objectifs fondamentaux[29] :

- protéger le réseau;
- réduire la vulnérabilité des systèmes informatiques et des applications aux menaces provenant du réseau;
- protéger les données pendant leur transmission dans le réseau.

Les cybercriminels essaient de trouver des faiblesses dans les dispositifs de protection de réseau connectés à Internet (p. ex. les pare-feu). Ces dispositifs protègent l'organisation contre les menaces provenant d'Internet. À défaut de pare-feu dans le périmètre du réseau pour protéger celui-ci contre les menaces sur Internet, les cybercriminels peuvent facilement voler la propriété intellectuelle de l'organisation et des renseignements de nature délicate.

[28] *United States of America v Baratov* (en anglais seulement), 2017 ONSC 2212 (CanLII).
[29] Centre canadien pour la cybersécurité. *Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada (ITSG-22)*, 2007 : 5.

L'adoption d'une méthode de défense en profondeur[30] réduira considérablement le nombre d'attaques Internet réussies dans le réseau interne d'une organisation. Les recommandations suivantes sont des recommandations en matière de sécurité du réseau :

- Acheter un pare-feu de la prochaine génération offrant les services de sécurité supplémentaires suivants :
    - le filtrage des sites Web renfermant des éléments malveillants;
    - la protection contre les virus sur Internet et contre les logiciels malveillants qui peuvent infiltrer le réseau;
    - une technologie de prévention des menaces qui examine le trafic réseau pour détecter les vulnérabilités sur Internet et empêcher celles-ci d'infiltrer le réseau;
- Exiger l'authentification à facteurs multiples[31] pour tout accès à distance, notamment par RPV;
- Fractionner le réseau interne de l'organisation de sorte que les utilisateurs n'aient accès qu'aux services dont ils ont besoin dans le cadre de leur travail;
- Mettre en œuvre une solution de contrôle d'accès au réseau afin d'empêcher les systèmes informatiques inconnus de communiquer avec le réseau de l'organisation;
- Établir un comportement normal de base pour les dispositifs du réseau.

6.6 SÉCURITÉ DES RÉSEAUX SANS FIL

La connectivité sans fil offre l'avantage d'une mobilité et d'une productivité accrues, mais elle comporte également un certain nombre de risques critiques et de défis pour la sécurité. Il est extrêmement facile pour les cybercriminels d'utiliser les réseaux sans fil pour s'immiscer dans les organisations sans y mettre les pieds. Les signaux sans fil sont habituellement émis à l'extérieur de l'infrastructure physique d'un immeuble et ils contournent les mesures de protection traditionnelles du périmètre de sécurité filé, notamment les pare-feu et les systèmes de protection contre les intrusions.

Les cybercriminels obtiennent un accès illimité au réseau interne d'une organisation en installant des points d'accès sans fil dissimulés et non autorisés sur le réseau. Les employés mécontents ou d'autres personnes ayant des intentions malveillantes et prenant l'identité de sous-traitants autorisés sont habituellement responsables du placement de ces dispositifs.

Les recommandations suivantes sont des recommandations en matière de sécurité des réseaux sans fil :

- Veiller à ce que chaque dispositif sans fil connecté au réseau soit autorisé en raison d'un besoin professionnel légitime. Les organisations devraient refuser l'accès à tous les autres dispositifs sans fil, y compris les appareils Bluetooth;

[30] Une défense multicouche, par exemple deux pare-feu et l'installation d'antivirus sur les serveurs et sur les appareils des utilisateurs.

[31] Une authentification qui utilise deux ou plusieurs facteurs différents. Par exemple, (i) ce que vous connaissez (mot de passe, NIP), (ii) ce que vous détenez (dispositif d'identification cryptographique, jeton) ou (iii) ce que vous êtes (renseignements biométriques). Computer Security Resource Center du NIST (en anglais seulement).

- Effectuer une analyse de la vulnérabilité du réseau sans fil. Cette analyse permettra de déceler les vulnérabilités dans le réseau sans fil et tout dispositif non autorisé sur le réseau;
- Mettre en place un système de détection d'intrusions sans fil (SDISF) pour repérer les dispositifs sans fil non autorisés, et détecter les attaques et les compromissions réussies;
- Désactiver l'accès sans fil sur les systèmes informatiques qui ne répondent pas à des besoins professionnels légitimes, en accédant à la configuration matérielle de l'ordinateur qui est accessible au démarrage du système, et exiger un mot de passe de quiconque tente d'accéder à la configuration matérielle de l'ordinateur;
- Veiller à ce que la totalité du trafic sur le réseau sans fil soit protégée par chiffrement avancé, par exemple selon la norme de chiffrement avancé (norme AES), et à ce que l'accès Wi-Fi utilise une norme d'authentification avancée, par exemple la norme Wi-Fi Protected Access 2 (WPA2)[32];
- Veiller à ce que les réseaux sans fil utilisent des protocoles d'authentification sécurisée comme Extensible Authentication Protocol-Transport Layer Security (EAP/TLS);
- Désactiver les fonctions du réseau sans fil entre pairs pour les clients qui ont un accès sans fil;
- Désactiver l'accès périphérique sans fil des dispositifs (notamment les appareils Bluetooth), à moins qu'il n'existe un besoin professionnel légitime.

6.7 ACCÈS À DISTANCE

De nombreuses technologies sont maintenant accessibles pour garantir un accès protégé aux systèmes informatiques d'une organisation. Tout comme les technologies sans fil, il est essentiel que l'accès à distance fasse l'objet d'une gestion et d'une maintenance constantes pour éviter que les utilisateurs non autorisés aient accès au réseau de votre organisation.

Les recommandations suivantes sont des recommandations en matière d'accès à distance sécurisé[33] :

- Mettre en œuvre une politique d'accès à distance et former le personnel pour qu'il la respecte;
- Utiliser seulement des technologies par RPV sécurisé pour l'accès à distance;
- Configurer le RPV sécurisé de manière à interdire la tunnellisation partagée;
- Surveiller et consigner toutes les sessions ouvertes par accès à distance;
- Exiger l'authentification à facteurs multiples pour toute session ouverte par accès à distance.

[32] Voir les recommandations actuelles en matière de protocoles de sécurité à l'adresse https://www.us-cert.gov/ncas/tips/ST18-247 (en anglais seulement).
[33] Sécurité publique Canada. *La sécurité des systèmes de contrôle industriels*, Pratiques exemplaires recommandées, 2012.

Étude de cas (2019) : Des acteurs d'un État-nation piratent les réseaux de deux municipalités aux É.-U.[34]

Le FBI a lancé une alerte de sécurité à ses partenaires du secteur privé au début de 2020 pour les aviser que des pirates informatiques d'un État-nation s'étaient introduits dans les réseaux de deux municipalités des États-Unis en 2019.

Les pirates ont profité de la vulnérabilité CVE-2019-0604 des serveurs Microsoft SharePoint pour exécuter leur attaque. Le FBI précise qu'une fois que les pirates informatiques se sont introduits dans ces réseaux, ils se sont livrés à des activités malveillantes : exfiltration des renseignements des utilisateurs, élévation des privilèges administratifs et dépôt de *webshells* pour assurer l'accès à distance et par la porte arrière. Le FBI a dit croire qu'il s'agissait d'acteurs non identifiés d'un État-nation en raison du degré de sophistication de la compromission et des tactiques, techniques et procédures (TTP) utilisées.

Les attaques contre des municipalités américaines ne sont pas des cas isolés, et ces attaques ne sont pas les premières à exploiter la vulnérabilité CVE-2019-0604 des serveurs SharePoint. Tout au long de l'année 2019, cette vulnérabilité en particulier de SharePoint a été l'un des défauts de sécurité les plus exploités, tant par des cybercriminels motivés par l'appât du gain que par des groupes de cyberespionnage parrainés par un État-nation.

Les premières attaques détectées ont été découvertes par le Centre canadien pour la cybersécurité à la fin avril, au moment où l'organisme a sonné l'alerte. Le National Cyber Security Center (NCSC) saoudien confirmait une vague d'attaques semblable une semaine plus tard, au début mai.

6.8 SÉCURITÉ DES POINTS TERMINAUX

Les employés qui ont accès aux ressources ou aux locaux de l'organisation, ou qui bénéficient d'un accès à distance devraient utiliser seulement le matériel d'accès approuvé par la société[35]. Outre les indications énoncées à la section 6.9 *Protection des systèmes d'information*, tous les utilisateurs devraient suivre les recommandations ci-après[36] :

- Veiller à ce que toutes les mises à jour se fassent automatiquement pour que la solution de blocage des logiciels malveillants soit à jour et effectue une surveillance en permanence des activités malveillantes;
- Ne pas transférer de renseignements vers des destinations non autorisées (p. ex. dispositifs de stockage non autorisés, Hotmail, Gmail, DropBox);
- Ne pas connecter de dispositifs non autorisés aux ordinateurs de la société (p. ex. téléphones intelligents, clés USB et lecteurs de disque dur);

[34] ZDNet. *FBI: Nation-state actors have breached two US municipalities* (en anglais seulement), 16 janvier 2020.
[35] Voir l'analyse sur les mesures de sécurité appropriées à la section 6.10 *Apportez votre équipement personnel de communication* si cette politique a été adoptée.
[36] Gouvernement du Canada. *Guide Pensez cybersécurité pour les petites et moyennes entreprises*.

- Ne pas brancher de clés USB de la société sur des appareils non approuvés (p. ex. ordinateurs portables, ordinateurs personnels, téléviseurs intelligents);
- Se méfier des appels téléphoniques, des visites et des courriels de personnes qui vous posent des questions sur les employés, leur famille et des dossiers de travail de nature délicate;
- Ne pas répondre aux courriels douteux et ne pas cliquer sur les liens dans les courriels douteux;
- Ne pas laisser son ordinateur portable ou des appareils semblables dans une aire publique, même un instant;
- Veiller à garder les renseignements confidentiels à son écran à l'abri du regard des curieux;
- Éviter les connexions Wi-Fi inconnues et gratuites.

6.9 PROTECTION DES SYSTÈMES D'INFORMATION

Les systèmes informatiques doivent être protégés contre toute tentative de piratage, notamment les ordinateurs qui sont utilisés pour accéder à distance aux ressources de la société. Les recommandations suivantes sont des recommandations en matière de protection des systèmes d'information contre les cybermenaces tels les rançongiciels et les virus :

- Mettre en œuvre des processus de sauvegarde et de récupération, et effectuer périodiquement des sauvegardes de vos systèmes;
- Mettre en place une solution de blocage des logiciels malveillants qui surveille en permanence les postes de travail, les serveurs et les appareils mobiles à l'aide de logiciels antivirus et anti-espion et de pare-feu;
- Mettre en place une solution de blocage des logiciels malveillants qui comprend une fonction IPS en mode hôte;
- Mettre en œuvre une politique pour contrôler tous les accès à des supports amovibles;
- Limiter l'utilisation des dispositifs externes, p. ex. les clés USB, aux personnes qui ont des besoins professionnels légitimes;
- Utiliser les pare-feu personnels intégrés dans Windows et les systèmes UNIX;
- Effectuer une analyse de tous les supports pour éliminer les logiciels malveillants avant de les importer sur le système de l'organisation;
- Installer toutes les mises à jour de sécurité des applications et des systèmes d'exploitation, notamment celles offertes par la fonction intégrée de mise à jour de Windows;
- Surveiller l'utilisation et les tentatives d'utilisation de dispositifs externes;
- Donner aux utilisateurs à distance l'accès aux ressources de l'organisation au moyen d'un RPV sécurisé et d'une authentification à facteurs multiples.

Plusieurs fournisseurs vendent à des prix abordables des solutions intégrées de sécurité des points terminaux pour les systèmes informatiques personnels et ceux de petites entreprises et de sociétés.

6.10 APPORTEZ VOTRE ÉQUIPEMENT PERSONNEL DE COMMUNICATION

Le concept *Apportez votre équipement personnel de communication* (AVEC) est de plus en plus populaire dans le milieu des affaires. Cette locution désigne la politique qui permet aux employés d'utiliser leurs propres appareils (p. ex. leur ordinateur portable, leur téléphone intelligent et leur tablette) pour accéder aux applications et aux données de la société. Bien que cette politique présente de véritables avantages, elle comporte également d'importants risques. Par exemple :

- la perte d'un appareil personnel qui renferme des renseignements de l'entreprise;
- l'installation d'applications malveillantes;
- la communication de renseignements de l'entreprise à des personnes non autorisées, p. ex. lorsque des membres de la famille ou des amis utilisent aussi l'appareil;
- le non-respect possible des lois et règlements en matière de confidentialité des données de l'employé si la politique n'est pas mise en œuvre adéquatement.

Une entreprise doit évaluer les risques et demander un avis juridique avant de décider si elle autorisera le concept AVEC et comment elle gérera les risques qui y sont associés. Comme l'application du concept AVEC en milieu de travail a donné lieu à de nombreux cas d'atteinte à la protection des données[37], il est important que les entreprises établissent une politique AVEC complète. À tout le moins, cette politique devrait préciser[38] :

- à qui la politique s'applique (p. ex. le personnel, les sous-traitants);
- quels appareils peuvent être utilisés (p. ex. des ordinateurs personnels, des tablettes);
- à quels services ou renseignements elle donne accès (p. ex. les courriels, les calendriers, des personnes-ressources);
- les obligations de l'employeur et des membres du personnel (y compris les mesures de sécurité qui doivent être adoptées);
- les applications qui peuvent et ne peuvent pas être installées (p. ex. pour la navigation dans les médias sociaux, l'échange de données, l'ouverture de fichiers);
- la façon dont on peut accéder aux applications et aux données. Idéalement, les dispositifs non vérifiés devraient avoir accès aux applications et aux renseignements de l'entreprise par l'entremise d'un ordinateur personnel virtuel. Il y a des sociétés qui offrent des produits de bureau virtuel qui conviennent bien à une mise en œuvre sécurisée de la politique AVEC;
- l'aide et le soutien qu'offre le personnel des TI;
- les pénalités pour toute non-conformité (p. ex. la perte des privilèges que confère la politique AVEC et d'autres procédures disciplinaires).

[37] Trend Micro. *Mobile Consumerization Trends & Perceptions: IT Executive and CEO Survey* (en anglais seulement), 2012.
[38] Fraud Advisory Panel. *Bring your own device (BYOD) policies* (en anglais seulement), 2014.

6.11 GESTION DES APPAREILS MOBILES

Le logiciel de gestion des appareils mobiles est un logiciel qui sécurise les téléphones intelligents, les tablettes et les autres points terminaux et assure le respect des politiques concernant ces appareils. Ce logiciel a pour but d'optimiser la fonctionnalité et la sécurité des appareils mobiles au sein de l'organisation tout en protégeant le réseau de celle-ci. Il s'agit d'une protection particulièrement importante pour les téléphones intelligents et les tablettes qui accèdent aux services infonuagiques de courriel et de fichiers.

Voici les principaux services offerts :

- l'inventaire et la localisation des appareils;
- la distribution des applications – la façon dont les applications mobiles sont fournies aux utilisateurs et la façon pour les utilisateurs de s'abonner à leur utilisation;
- le nettoyage à distance dans le cas de la perte ou du vol d'un appareil, ou dans le cadre du processus de gestion du départ d'un employé.

Les principales politiques qui doivent être élaborées pour les appareils sont les suivantes :

- Application des règles relatives aux mots de passe – veiller à ce que ces règles soient suivies;
- Établissement d'une liste blanche et d'une liste noire des applications – contrôler explicitement les applications qui peuvent être utilisées et celles qui ne devraient pas l'être;
- Application des règles relatives au chiffrement des données – s'assurer que ces règles sont suivies;
- Double authentification – appliquer l'authentification à facteurs multiples pour l'accès aux services et aux renseignements clés.

6.12 SAUVEGARDE ET REPRISE DES ACTIVITÉS

Un plan de sauvegarde est essentiel pour toute organisation. Les sauvegardes garantissent que l'organisation pourra reprendre rapidement ses activités, car les fichiers perdus ou endommagés peuvent être récupérés. Les sauvegardes effectuées en temps opportun sont particulièrement essentielles lorsque l'organisation reprend ses activités après une attaque menée au moyen d'un logiciel malveillant. Les petites et moyennes entreprises ont accès aux options de sauvegarde suivantes :

- **Lecteur de disque dur USB pour ordinateur portable ou personnel**
  Un processus automatisé peut effectuer une sauvegarde périodique de chaque système d'information.

- **Serveur**
  Les données importantes des utilisateurs peuvent être sauvegardées sur un serveur connecté au réseau. Un processus automatisé du serveur sauvegarde ensuite

périodiquement les données des utilisateurs. L'exécution d'une copie de sauvegarde devrait alterner avec celle d'une copie à conserver à l'extérieur des locaux.

- **Nuage**
  Les services de sauvegarde peuvent sauvegarder les fichiers dans le nuage. Les sociétés devraient examiner quelles données de quels territoires elles peuvent s'attendre à recevoir afin de respecter les règlements sur la protection des renseignements personnels. De plus, toutes les copies de sauvegarde devraient être chiffrées.

6.13 GESTION DES COMPTES D'UTILISATEUR ET CONTRÔLE DE L'ACCÈS

Les contrôles d'accès déterminent la façon dont les employés lisent leurs courriels, ont accès à leurs documents et se connectent à d'autres ressources du réseau. Les contrôles d'accès correctement appliqués garantissent la protection de la propriété intellectuelle et des données de nature délicate contre leur utilisation, leur communication et leur modification non autorisées.

Les recommandations suivantes sont des recommandations en matière de gestion des comptes d'utilisateur et de contrôle de l'accès :

- Mettre en œuvre un processus de gestion des comptes;
- Gérer centralement tous les comptes à l'aide d'un système de gestion des comptes;
- Configurer les appareils du réseau et les dispositifs de sécurité sur la base du système centralisé d'authentification;
- Limiter le nombre de comptes à privilèges à ceux qui ont un besoin professionnel légitime;
- Contrôler l'accès aux journaux d'audit du système informatique;
- Examiner tous les comptes du système et désactiver ceux qui ne peuvent pas être associés à un processus opérationnel ni à un responsable;
- Veiller à ce qu'une date d'échéance soit associée à chaque compte;
- Mettre en place un processus d'annulation immédiate de l'accès au système (désactivation des comptes) dès la cessation de la relation avec un employé ou un sous-traitant. La désactivation plutôt que l'élimination du compte permet de conserver une piste d'audit si une enquête se révélait nécessaire, par exemple;
- Obliger les utilisateurs à se connecter à nouveau après une période normale d'inactivité;
- Exiger que les mots de passe de tous les comptes d'employé soient des mots de passe forts qui renferment des lettres, des chiffres et des caractères spéciaux. Veiller à ce qu'ils soient modifiés aux 90 jours et que les 15 mots de passe précédents ne puissent pas être utilisés comme nouveau mot de passe;
- Exiger une authentification à facteurs multiples pour les comptes à privilèges ou les comptes donnant accès à des données de nature délicate ou à des systèmes informatiques contenant de telles données. L'authentification à facteurs multiples peut s'effectuer à l'aide de cartes à puces assorties de certificats, de mots de passe à usage unique ou de facteurs biométriques.

6.14 GESTION DES ACTIFS

Le contrôle géré des systèmes informatiques et des logiciels joue un rôle crucial dans le maintien de la sécurité de l'organisation. Il est essentiel de répertorier et de gérer tous les systèmes informatiques pour s'assurer que seuls les systèmes autorisés ont accès au réseau. Il est tout aussi important de veiller à ce que seuls des logiciels autorisés soient installés et que l'exécution de logiciels non autorisés soit interdite. Les mises à jour de sécurité ou les correctifs les plus récents ne sont généralement pas installés sur les applications et les systèmes non autorisés, parfois peu sûrs, qui sont donc plus susceptibles d'être exploités.

7. INTERVENTION EN CAS D'INCIDENT

La planification et la préparation en vue d'un incident de cybersécurité représentent l'un des plus grands défis d'une organisation. Lorsque survient un incident de cybersécurité, il faut prendre des mesures et atténuer, dès que possible, les menaces à la confidentialité, à l'intégrité et à l'accessibilité des actifs informationnels de l'organisation.

La gestion des cyberincidents permet d'atténuer les risques associés aux menaces internes et externes, et aide l'organisation à se conformer à la réglementation, le cas échéant. Une organisation doit être prête à gérer les incidents qui peuvent provenir de sources variées.

7.1 TERMES CLÉS

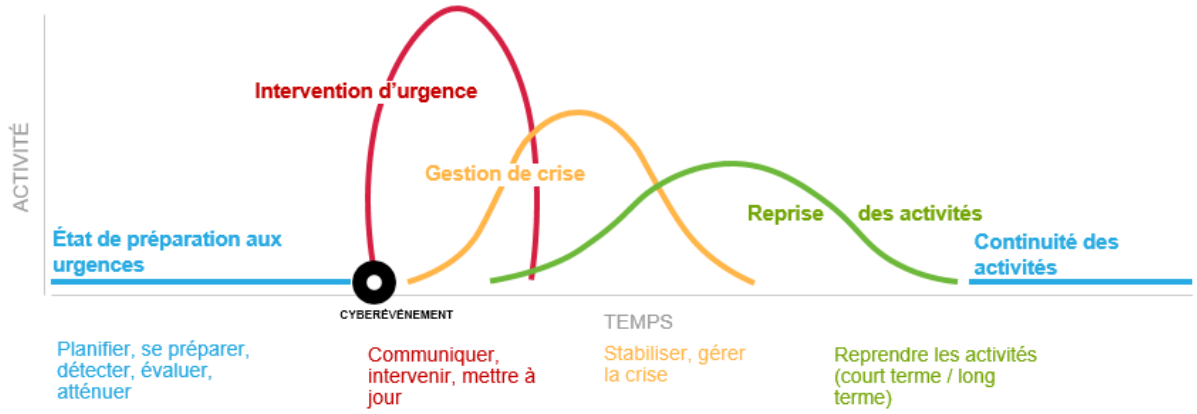
Le cadre de cybersécurité et les définitions utilisés dans le présent document s'alignent sur ceux du Plan de gestion des événements de cybersécurité du gouvernement du Canada (publié en 2018) et du Computer Security Incident Handling Guide (Special Publication 800-61, Revision 2, publiée en 2012) du National Institute of Standards and Technology (NIST) des États-Unis.

- **Compromission :** Il s'agit d'une brèche potentielle ou réelle de cybersécurité portant atteinte à la confidentialité, à l'intégrité et à la disponibilité de l'information numérique ou des actifs de technologie de l'information d'une entreprise.
- **Confidentialité :** La protection des renseignements contre toute communication non autorisée.
- **Intégrité :** L'assurance de l'exactitude, de l'exhaustivité et de l'authenticité des renseignements et des services.
- **Disponibilité :** La capacité à assurer les activités, les programmes et les services de l'entreprise.
- **Cyberévénement :** Tout événement *potentiellement préjudiciable* à la confidentialité, à l'intégrité ou à la disponibilité des actifs informationnels ou des actifs de technologie de l'information, notamment un cyberincident, qui résulte de menaces et de vulnérabilités.
- **Cyberincident :** Tout événement ayant provoqué une *véritable compromission* de la confidentialité, de l'intégrité ou de la disponibilité des actifs et qui résulte de menaces et de vulnérabilités.
- **Menace :** Toute possibilité d'événement de sécurité causé de manière délibérée, accidentelle ou naturelle qui pourrait compromettre les actifs de l'entreprise.
- **Vulnérabilité :** Une faiblesse dans les contrôles qui permet de détecter une menace, de s'en protéger, d'y réagir et de reprendre les activités et qui augmente la probabilité ou les répercussions d'une compromission pour l'organisation.

7.2 MODÈLE D'INTERVENTION EN CAS D'INCIDENT

Le plan d'intervention en cas de cyberincident peut être basé sur le modèle éprouvé du

système de commandement en cas d'incident (SCI)[39]. Le SCI établit une terminologie commune qui permet aux différents organismes d'intervention et d'aide en cas d'incident de travailler ensemble malgré des fonctions d'intervention variées et différents scénarios de danger.
Le diagramme ci-dessous illustre les phases de gestion des incidents, de la phase de préparation à la phase de reprise des activités. La courbe rouge au début de tout cyberévénement, où la confidentialité, l'intégrité ou la disponibilité des systèmes d'information ou de TI a déjà été compromise, indique qu'une intervention tactique sera coordonnée avant que le plan d'intervention en cas de cyberincident ne soit mis en œuvre. Dans tous les cas, l'équipe de la haute direction responsable de la surveillance des urgences a le pouvoir d'agir dans les limites de ses compétences afin d'assurer la protection des actifs informationnels et de TI de la société.
Le plan d'intervention en cas de cyberincident, représenté par la courbe jaune, doit être activé dès que les principaux objectifs du plan sont atteints. Le plan d'intervention en cas de cyberincident favorise la coordination efficace des tâches d'intervention et de reprise, et la communication avec les parties concernées.



7.3 STRUCTURE MODULAIRE

La structure organisationnelle du plan d'intervention en cas de cyberincident peut être adaptée à la nature, à l'ampleur et à la complexité des événements et des incidents à gérer. En fin de compte, la responsabilité de l'établissement et de l'expansion de la structure modulaire du plan d'intervention en cas de cyberincident relève du **chef des interventions**.

7.4 GESTION PAR OBJECTIFS

La gestion par objectifs est communiquée dans toute la structure du plan d'intervention en cas de cyberincident et comprend :

- L'établissement d'objectifs d'intervention en cas d'incident;
- L'élaboration de stratégies fondées sur les objectifs d'intervention en cas

[39] Le système de commandement en cas d'incident est un système de contrôle et de commandement sur place standard utilisé pour la gestion des incidents d'urgence et des événements planifiés.

d'incident;
- L'élaboration de plans, de procédures et de protocoles, et l'attribution des tâches;
- L'établissement de tactiques ou de tâches précises et mesurables pour diverses activités fonctionnelles d'intervention en cas d'incident, et le déploiement d'efforts pour l'accomplissement de ces tâches, afin de soutenir des stratégies définies;
- La consignation des résultats afin d'évaluer le rendement et de faciliter les mesures correctives;
- L'établissement d'un rythme d'intervention et de production de rapports par l'attribution de périodes opérationnelles pour les rapports internes.

7.5 PLAN D'ACTION EN CAS DE CYBERINCIDENT

Un plan d'action centralisé et coordonné en cas de cyberincident devrait orienter toutes les activités d'intervention. Le plan d'action en cas de cyberincident est un moyen concis et logique de regrouper et de communiquer l'ensemble des priorités, des objectifs, des stratégies et des tactiques liés à l'intervention en cas d'incident dans un contexte d'activités opérationnelles et de soutien.

Un plan d'action doit être élaboré pour tout cyberincident, mais il n'est pas nécessaire de rédiger un plan pour tous les cyberévénements. La décision de rédiger un plan revient au chef des interventions.

La plupart des opérations d'intervention initiales ne sont pas consignées dans un plan d'action en cas de cyberincident en bonne et due forme. Cependant, si un événement est susceptible de se prolonger au-delà d'une période opérationnelle, de devenir plus complexe ou de mobiliser des parties intéressées externes, il sera plus important de rédiger un plan d'action en cas de cyberincident pour assurer l'efficacité, l'efficience et la sécurité des activités. Par ailleurs, le plan d'action en cas de cyberincident contient une chronologie des décisions et des mesures prises en fonction de l'information disponible à ce moment-là.

7.6 ÉVENTAIL DE COMMANDEMENT GÉRABLE

Un éventail de commandement est essentiel à l'efficacité et à l'efficience d'une intervention en cas d'incident de cybersécurité. Les surveillants doivent être en mesure de surveiller adéquatement leurs subordonnés et d'exercer un contrôle sur eux, de communiquer avec toutes les ressources soumises à leur surveillance et de gérer ces ressources. Le type de cyberincident, la nature de la tâche, les dangers, la sécurité et la distance qui sépare le personnel des ressources sont tous des facteurs à prendre en considération lorsqu'il s'agit de déterminer l'éventail de commandement.

7.7 EMPLACEMENT DES INSTALLATIONS DÉSIGNÉES EN CAS D'INCIDENT

Le chef des interventions décidera de l'emplacement des installations selon les exigences de la situation. Normalement, les installations désignées en cas de cyberincident comprennent entre autres des postes de commandement, une cellule de crise pour les dirigeants et des aires de repos, selon les besoins.

7.8 GESTION EXHAUSTIVE DES RESSOURCES

Il est essentiel, dans le cadre d'une intervention d'urgence ou d'une intervention en cas de cyberincident, d'avoir un portrait précis et à jour des ressources qui sont utilisées, en grande partie pour avoir conscience de la fatigue ressentie par le personnel et pour gérer cette fatigue dans le but d'éviter l'épuisement professionnel. Les ressources à répertorier sont les membres du personnel, les équipes, le matériel, les fournitures et les installations qui peuvent ou qui pourraient être affectées ou distribuées.

7.9 COMMUNICATIONS INTÉGRÉES

La communication des données et les communications verbales lors d'interventions en cas de cyberincident sont facilitées par l'élaboration et l'utilisation d'un plan de communication commun, et par des processus et une architecture de communication interexploitables.
Une méthode de communication intégrée permet d'établir un lien entre les unités opérationnelles et les unités de soutien mobilisées; elle fait en sorte que tous les intervenants connaissent la situation. Le plan de préparation devrait énoncer le matériel, les systèmes et les protocoles nécessaires à l'intégration des communications de données et des communications verbales.

7.10 ÉTABLISSEMENT DU COMMANDEMENT ET TRANSFERT DE COMMANDEMENT

La fonction de commandement doit être établie clairement dès le début des activités liées au cyberincident, mais elle peut être déléguée si la situation d'intervention se prolonge. Lorsque le commandement est délégué, il faut donner des instructions pour maintenir la sécurité et l'efficacité des activités.

7.11 CHAÎNE DE COMMANDEMENT

La chaîne de commandement et une voie hiérarchique ordonnée au sein de l'équipe d'intervention en cas de cyberincident. Elle clarifie les liens hiérarchiques et élimine toute confusion que pourraient causer des directives multiples ou contradictoires.

7.12 DÉPLOIEMENT

Les ressources doivent intervenir seulement lorsqu'on le leur demande ou lorsqu'elles sont déployées par l'autorité compétente. Les ressources qui ne sont pas mobilisées doivent

s'abstenir de se présenter spontanément afin d'éviter de surcharger le bénéficiaire de l'aide et d'aggraver les problèmes de responsabilité.

7.13 GESTION DE L'INFORMATION ET DES RENSEIGNEMENTS

L'équipe d'intervention en cas de cyberincident doit prévoir un processus pour la collecte, l'analyse, l'évaluation, l'échange et la gestion de l'information et des renseignements qui ont trait à un incident.

8. ORGANISATION ET OPÉRATIONS LORS D'UNE INTERVENTION EN CAS D'INCIDENT

Tous les cyberincidents donnent lieu à des tâches semblables en matière d'intervention. Les problèmes provoqués par le cyberincident doivent être décelés et évalués, un plan de gestion de ces problèmes doit être élaboré et exécuté, et les ressources nécessaires doivent être acquises. Le plan d'intervention en cas de cyberincident fournit la structure permettant de gérer efficacement les tâches d'intervention communes ci-après :

- Assurer un leadership et mettre en place une structure organisationnelle pour réduire au minimum les répercussions éventuelles ou réelles d'un cyberincident;
- Fixer des buts et des objectifs, et établir des stratégies et des tactiques;
- Élaborer des plans et communiquer clairement ces plans à tous les intervenants concernés;
- Gérer l'information concernant les incidents de cybersécurité, les menaces et les vulnérabilités, et contribuer à ce que cette information soit rapidement transmise à toutes les parties intéressées, à l'interne comme à l'externe;
- Assurer un suivi des circonstances du cyberincident, de la phase initiale d'escalade à la phase de désescalade, de résolution et d'examen après l'incident;
- Maintenir un éventail de commandement efficace et demander des ressources supplémentaires au besoin;
- Consigner les décisions prises et les activités exercées relativement à l'intervention en cas de cyberincident.

Pour que toute intervention en cas d'incident important soit efficace et que les tâches soient accomplies, le travail doit être divisé. La structure du plan d'intervention en cas de cyberincident s'articule autour de cinq activités de gestion principales :

1. **Commandement en cas d'incident**
   Établissement des objectifs et des priorités, et responsabilité à l'égard de l'incident.
2. **Opérations d'affaires**
   Exécution des opérations tactiques en vue de l'application du plan. Établissement des objectifs tactiques, et organisation et gestion des ressources.
3. **Planification**
   Élaboration du plan d'action qui permettra l'atteinte des objectifs, et collecte et évaluation de l'information. Maintien de l'état des ressources.
4. **Logistique**
   Soutien en vue de répondre aux besoins engendrés par l'incident. Allocation des ressources et des autres services nécessaires dans ce contexte.
5. **Finances et administration**
   Suivi des coûts liés à l'incident, comptabilité, approvisionnement, gestion

des temps et analyse des coûts.

Ces cinq activités de gestion principales sont à la base de la structure du plan d'intervention en cas de cyberincident.

8.1 CINQ PHASES PRINCIPALES DU PROCESSUS DE PLANIFICATION

Comprendre la situation
La première phase comprend la collecte, la consignation, l'analyse et la présentation de l'information sur la situation, les ressources et l'incident potentiel d'une manière qui favorisera :

- la connaissance ciblée de l'ampleur, de la complexité et des répercussions potentielles de l'incident;
- la confirmation des ressources requises pour l'élaboration et l'exécution du plan d'action en cas de cyberincident.

Établir les objectifs en cas d'incident et adopter une stratégie
La deuxième phase est centrée sur la conception et la priorisation d'une intervention mesurable en cas d'incident, et l'adoption d'une stratégie appropriée. Les objectifs et la stratégie doivent être conformes aux obligations juridiques et aux objectifs de la direction. D'autres stratégies raisonnables qui permettraient de réaliser les objectifs généraux en cas d'incident sont proposées, étudiées et évaluées dans le but de définir la stratégie la plus appropriée pour la situation. Le préjudice public, les coûts estimés et divers facteurs d'ordre réglementaire, juridique et politique sont tous des critères d'évaluation.

Élaborer un plan
La troisième phase consiste à déterminer l'orientation tactique et les besoins précis en matière de ressources, de réserves et de soutien pour l'exécution des stratégies et des tactiques sélectionnées durant la période opérationnelle. Avant chaque réunion de l'équipe d'intervention en cas de cyberincident, chaque membre de l'équipe est chargé de recueillir des renseignements pour soutenir le plan proposé.

Préparer et distribuer le plan
La quatrième phase consiste à préparer le plan dans une forme appropriée au niveau de complexité de l'incident. Pour l'intervention initiale, il peut prendre la forme d'un aperçu bien préparé qui est communiqué oralement dans le cadre d'une séance d'information. Pour la plupart des incidents qui se prolongent sur plusieurs périodes opérationnelles, le plan est alors rédigé conformément aux procédures et à l'aide du modèle standard de plan d'action en cas de cyberincident.

Exécuter, évaluer et revoir le plan

Le processus de planification repose notamment sur l'obligation d'exécuter et d'évaluer les activités prévues, et de vérifier l'exactitude des renseignements qui serviront à planifier les périodes opérationnelles ultérieures. L'équipe d'intervention en cas de cyberincident devrait comparer périodiquement les progrès prévus avec les progrès réels. Tout écart et tout nouveau renseignement devraient être pris en compte à la première étape du processus qui sert à modifier le plan en cours ou à élaborer le plan pour la période opérationnelle subséquente.

9. ÉCHANGE D'INFORMATION ET SIGNALEMENT DES INFRACTIONS

9.1 AVIS D'ATTEINTE À LA VIE PRIVÉE

Les plans d'intervention en cas d'incident doivent prévoir des directives claires concernant la gestion de toute atteinte éventuelle à la protection des données, y compris des directives sur la transmission d'un avis à tous les organismes de réglementation concernés. Voir les principaux facteurs juridiques à la section 3.4.

9.2 ÉCHANGE D'INFORMATION

Les cybermenaces sont présentes à l'échelle planétaire et elles ne se limitent pas à une société, à un secteur ou à un marché. L'échange d'information est un élément essentiel d'un programme de cybersécurité efficace et un outil indispensable pour atténuer les cybermenaces. L'échange d'information se fait aux niveaux stratégiques, tactiques, opérationnels et techniques, de même qu'à toutes les phases du cycle d'intervention en cas d'incident. Il transcende les frontières des domaines public et privé. Les doutes quant à l'intégrité d'un participant au marché peuvent rapidement s'étendre à d'autres et avoir une incidence sur la confiance globale des investisseurs. Enfin, les renseignements échangés peuvent être de nature délicate, ce qui peut être nuisible à une organisation, tout en étant très utile à d'autres[40].

Il existe, pour les courtiers membres, diverses possibilités et tribunes d'échange proactif des renseignements. Les communautés d'échange de renseignements se fondent sur le principe suivant : les mesures de cybersécurité efficaces constituent un bien collectif, et un incident de sécurité au sein d'une institution est un premier avertissement pour la communauté.

9.3 GESTION DES RISQUES LIÉS AUX FOURNISSEURS ET À L'EXTERNALISATION

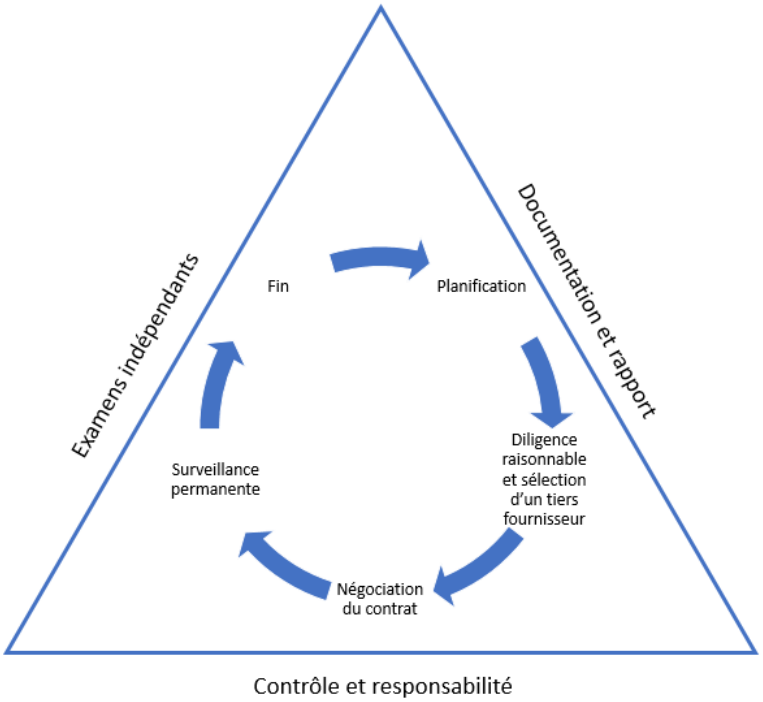
Le recours à un tiers fournisseur pour certains services clés continue d'être une stratégie importante pour bien des sociétés. Les courtiers membres qui externalisent certains services héritent des pratiques de sécurité de ces fournisseurs. Il faut prendre certaines précautions pour s'assurer que les activités et les risques sont totalement transférés aux fournisseurs et gérés par eux.

Les éléments essentiels d'un programme de gestion des risques liés aux fournisseurs et à l'externalisation sont notamment les suivants :

- Le classement des fournisseurs en fonction des risques;
- L'établissement de politiques claires que les fournisseurs devraient respecter;
- L'intégration de conditions explicites dans les contrats;
- L'établissement d'un programme visant à vérifier le rendement des fournisseurs.

[40] Luiijf, E. et A. Kernkamp. *Sharing Cybersecurity Information: Good Practice Stemming from the Dutch Public-Private-Participation Approach* (en anglais seulement), mars 2015.

L'Office of the Comptroller of the Currency (OCC) des États-Unis a élaboré un excellent cadre pour la création d'un programme efficace de gestion des risques liés aux fournisseurs (voir la Figure 1 ci-dessous).



Source : OCC

Figure 1 – Cycle de la gestion des risques que posent les tiers, Office of the Comptroller of the Currency (OCC)

Toute gestion adéquate des fournisseurs commence dès la conclusion du contrat. Ce modèle de cycle de vie indique les principales étapes que sont la planification préliminaire, la diligence raisonnable et la négociation et qui permettent de s'assurer que les fournisseurs respectent les politiques de sécurité de l'entreprise. Même si la surveillance permanente est essentielle, il est tout aussi important de planifier la fin de la relation pour que l'accès aux réseaux soit interrompu et que les données confidentielles soient retournées à l'entreprise.

Les entreprises devraient envisager une gestion des risques liés aux fournisseurs par niveau, le premier étant réservé aux relations posant le plus grand risque. Normalement, il s'agira des fournisseurs de services administratifs et ceux de la salle des marchés.

La stratification des fournisseurs peut être abordée sous l'angle des facteurs suivants :

Risques liés au service

- Volume d'opérations financières traitées
- Concentration associée aux services
- Risque lié au caractère sensible des données auxquelles le fournisseur pourrait avoir accès
- Risque de conformité et risque réglementaire en lien avec le service
- Impact financier et conséquences pour la clientèle

Risques liés au fournisseur

- Emplacement du fournisseur (sous réserve des lois et règlements multinationaux, de la règle d'exonération, etc.)
- Atteintes antérieures à la sécurité ou à la protection des données
- Ampleur des services externalisés au fournisseur
- Historique du rendement

Lacunes courantes présentées par les tiers fournisseurs

- Plan de gestion de l'intervention en cas d'incident
- Connaissance insuffisante de la sécurité
- Prévention de la perte de données
- Chiffrement des données stockées et en transit
- Blocage des privilèges d'administrateur
- Essais de vulnérabilité ou tests de pénétration

Méthodes courantes d'évaluation des tiers fournisseurs

- Questionnaires inclus dans les demandes de propositions[41].
- Demandes de documents aux fournisseurs éventuels[42]
- Attestations délivrées par un tiers comme ISO 27001, SOC 2, ISO 27017, ISO 27018
- Évaluations administratives pour évaluer les renseignements demandés
- Visites sur place, s'il y a lieu, par des spécialistes internes ou externes
- Tests de pénétration des fournisseurs potentiels

La gestion des risques liés aux fournisseurs devrait être intégrée dans le programme de gestion des risques de l'organisation et comporter des processus établis, reproductibles et uniformes pour tous les services de l'organisation.

9.4 INFONUAGIQUE

L'infonuagique désigne l'accès à des données et à des programmes stockés sur Internet plutôt que sur un ordinateur de bureau[43]. L'infonuagique comporte de nombreux avantages, mais également des risques semblables aux risques associés à l'externalisation à des tiers fournisseurs. En fait, un grand nombre de tiers fournisseurs offrent leurs services à partir du nuage.

Les services infonuagiques offerts varient des sauvegardes à l'échange et à la distribution de fichiers en passant par l'archivage, et bien plus encore. La principale activité d'un fournisseur de services infonuagiques est le stockage d'applications critiques et de données sensibles. Par conséquent, la sécurité et la confidentialité des données sont les principales préoccupations de

[41] Voir le modèle de questionnaire d'évaluation des fournisseurs à l'annexe B Le Guide de pratiques
[42] Le modèle de questionnaire d'évaluation des fournisseurs à l'annexe B Le Guide de pratiques donne des exemples du type de documents dont il est question.
[43] Journal de Montréal. *Qu'est-ce que l'infonuagique?*, septembre 2016.

la plupart des entreprises qui envisagent de recourir à cette option. Les entreprises doivent tenir compte des risques et des menaces inhérentes, en plus des risques qu'elles sont disposées à assumer.

Ces risques comprennent la non-disponibilité des données ou des applications, la perte de données, et le vol et la divulgation non autorisée de renseignements de nature délicate. En plus de suivre les directives sur l'atténuation des risques énoncées à la section portant sur la gestion des fournisseurs, les entreprises qui envisagent le recours à des services infonuagiques devraient trouver un fournisseur qui répond aux critères suivants[44] :

- Le fournisseur possède d'importants antécédents dans le domaine des services infonuagiques et peut fournir des références professionnelles solides;
- Il décrit clairement ses contrôles d'atténuation des risques – contrôles liés à la sécurité, à la disponibilité, à l'intégrité du traitement, à la confidentialité et à la protection des renseignements personnels;
- Le fournisseur propose des accords clairs sur les niveaux de service, particulièrement en ce qui concerne :
    - la disponibilité;
    - la notification des incidents potentiels;
    - sa réponse aux billets des clients;
- Le fournisseur autorise les audits et les vérifications de ses contrôles;
- Le fournisseur est accrédité ou reconnu par au moins une autorité du domaine des normes de sécurité;
- Ses procédures de sauvegarde, ses plans de poursuite des activités et ses plans de reprise après sinistre répondent aux exigences de votre entreprise;
- Le fournisseur stocke les renseignements et les gèrent conformément aux lois et règlements principaux sur la protection des renseignements personnels, particulièrement dans les territoires où sont stockées et sauvegardées les données;
- Il facilite le rapatriement des renseignements de votre entreprise et des clients à votre entreprise à la fin de l'accord.

9.5 FOURNISSEURS DE SERVICES GÉRÉS

De nombreuses organisations, plus particulièrement les petites et moyennes entreprises, font appel à un fournisseur de services gérés pour leurs besoins de TI et de sécurité. Ces fournisseurs de services gérés donnent accès à une expertise rare, assurent une surveillance 7 jours sur 7, 24 heures sur 24, et offrent des capacités supplémentaires en matière d'intervention.

Les services offerts par ces fournisseurs varient des solutions ponctuelles, comme la gestion des pare-feu, la surveillance du périmètre et la protection des points terminaux, aux services de sécurité complets pour l'ensemble des appareils et des renseignements d'une organisation. Les courtiers membres devraient bien réfléchir à ce qu'ils souhaitent externaliser. En répondant aux

[44] ISACA. *Security Considerations for Cloud Computing*, 2012.

questions suivantes, les sociétés pourront déterminer plus facilement quand externaliser les services de sécurité et quels fournisseurs répondent le mieux à leurs besoins bien précis :

1. Quelles sont les responsabilités respectives de part et d'autre quant à la protection des données de notre société? Les rôles et responsabilités sont-ils définis clairement à l'aide de mesures de la responsabilité?
2. Quel est le processus de mise en place des services informatiques? Quelles mesures seront prises pour offrir les services externalisés et veiller à ce qu'ils soient fournis aux niveaux prévus? À quel investissement de temps et d'efforts s'attend-on de notre société?
3. Quel accès notre société aura-t-elle aux données enregistrées par les services de sécurité et aux activités du personnel de sécurité?
4. Qui aura accès à notre société et dans quelles circonstances? Quelle est la piste d'audit du personnel? Quel type d'accès aux données de notre société le personnel a-t-il? Quelle est la configuration des services qui nous sont offerts?
5. Où les données de notre entreprise seront-elles stockées? Dans quels pays? Et où les copies de sauvegarde de nos données seront-elles stockées?
6. Quel est votre niveau de service quant à la disponibilité des services que vous offrez?
7. Dans quelle mesure votre expertise est-elle reconnue et confirmée? Quelles accréditations votre société possède-t-elle, et quels sont les titres professionnels de vos employés?
8. À quel niveau de soutien puis-je m'attendre pour les clients?
9. Quel est votre niveau de service pour la notification des incidents? Quels services d'enquête, de confinement et de correction offrez-vous en cas d'incident?
10. Quel est le processus en place pour mettre fin à la relation? Quels services continuerez-vous de fournir à notre société durant la transition? Quelles données notre société peut-elle rapatrier? Quelles sont les données qui seront détruites? Quelle sorte de vérification par un tiers sera effectuée pour confirmer que tous les processus de sortie ont été suivis adéquatement?

9.6 OUTILS COMPLETS DE BUREAUTIQUE ET DE COLLABORATION

Certaines sociétés offrent des ensembles complets d'outils de bureautique et de collaboration (messagerie électronique, documents, feuilles de calcul, présentations, clavardage, réunions d'équipe, etc.) ainsi que le stockage et la gestion des fichiers.

Des solutions de sécurité complètes sous-tendent et soutiennent les services offerts :

- Protection et surveillance du périmètre, et alertes;
- Chiffrement des données stockées et en transit;
- Authentification à facteurs multiples;
- Conformité avec une vaste gamme de lois, de règlements et d'attestations.

Les services de sécurité moyenne et de sécurité élevée offrent habituellement de meilleurs services de sécurité et une plus grande protection, y compris la protection des données par

niveau, la protection de la confidentialité, l'investigation électronique et des capacités d'intervention améliorées en cas d'incident. Ces services permettent aux sociétés d'externaliser non seulement leurs activités de TI, par exemple un soutien pour les courriels et les serveurs de fichiers, mais également leurs opérations de sécurité et leur gestion de la sécurité. Tout comme les fournisseurs de services gérés, ces sociétés centralisent l'expertise des rares ressources qui existent sur le marché.

Les sociétés peuvent externaliser une grande partie de ces services ainsi que le soutien et la maintenance pour ces services, mais elles ne peuvent confier à un tiers la gouvernance opérationnelle et stratégique. Dans ces modèles, la sécurité est une responsabilité partagée. Les fournisseurs fournissent l'infrastructure et les services de base, tandis que les sociétés sont responsables de la configuration et de l'exploitation de l'information, ainsi que des applications, des appareils et des utilisateurs. Les sociétés conservent la responsabilité de certaines activités clés :

- La création et la suppression de l'accès des utilisateurs;
- La gestion des appareils, en particulier des appareils mobiles;
- La sensibilisation et la formation des utilisateurs;
- La classification et la manipulation des données;
- Le chiffrement des données, particulièrement des données stockées.

9.7 GOUVERNANCE HYBRIDE

De nombreuses sociétés optimisent leurs opérations et leurs budgets en adoptant un modèle hybride. Certains renseignements et services sont dans le nuage, et d'autres demeurent sur place ou sont stockés dans les centres de données de tiers. Les responsabilités en matière de gouvernance demeurent les mêmes, mais des processus de gouvernance doivent être mis en place et exécutés. Dans le cas d'une solution hybride, l'accent est mis sur ce qui suit :

- Assurer l'interopérabilité des renseignements et des processus sur place et dans le nuage, et veiller à ce qu'aucun risque opérationnel ou risque pour la sécurité ne soit introduit;
- Veiller à ce que les rôles et responsabilités soient bien définis au sein de la société en ce qui concerne les renseignements, les services et les processus sur place et dans le nuage;
- Assurer l'intégration des plans, des processus et des capacités d'intervention en cas d'incident et de continuité des activités.