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

juno RISK SOLUTIONS

Guide de pratiques exemplaires en matière de cybersécurité

À l'intention des courtiers membres de l'OCRCVM

Table des matières

Sommaire

Compte tenu de l'importance de la gestion proactive des cyberrisques pour garantir la stabilité des sociétés réglementées par l'OCRCVM, l'intégrité des marchés financiers canadiens et la protection des intérêts des investisseurs, le présent document propose un cadre de cybersécurité volontaire, c'est-à-dire un ensemble de normes et de pratiques exemplaires du secteur pour aider les courtiers membres de l'OCRCVM à gérer les risques en matière dee cybersécurité.

Les directives volontaires énoncées dans ce guide permettront aux courtiers membres de personnaliser et de quantifier les ajustements apportés à leurs programmes de cybersécurité à l'aide de techniques et de contrôles efficients de gestion des risques. Les courtiers membres de moindre taille comprendront mieux la façon d'appliquer des mesures de sécurité de base à leurs systèmes informatiques et à leurs réseaux.[1] Dans le cas des courtiers membres de plus grande envergure, le guide propose une démarche économique pour protéger les systèmes informatiques en fonction des besoins de l'organisation, sans ajouter aux exigences réglementaires.

Les points saillants du rapport sont les suivants :

- Un cadre de saine gouvernance reposant sur un leadership vigoureux est essentiel pour la cybersécurité efficace à la grandeur de l'organisation. La mobilisation du conseil d'administration et de la haute direction est primordiale pour la réussite des programmes de cybersécurité, tout comme une chaîne de reddition de comptes précise.

- Une équipe bien formée peut représenter la première ligne de défense contre les cyberattaques. Une formation efficace aidera à réduire la probabilité d'attaque réussie en transmettant aux membres du personnel bien intentionnés des connaissances qui leur permettront d'éviter de devenir des vecteurs d'attaque par inadvertance (par exemple, en téléchargeant involontairement des programmes malveillants).

- Le niveau de complexité des contrôles techniques appliqués par une organisation dépend largement de sa situation. Bien qu'une petite organisation puisse ne pas être en mesure de mettre en œuvre la totalité des contrôles, les stratégies proposées peuvent servir de fonction d'analyse comparative essentielle pour bien faire comprendre les vulnérabilités par rapport aux normes sectorielles.

- Les courtiers membres de l'OCRCVM ont habituellement recours à des fournisseurs de services indépendants qui exigent l'accès aux renseignements de nature délicate de l'organisation ou de ses clients, ou aux systèmes de l'organisation. Parallèlement,

[1] Les clients, les employés et les partenaires actuels et/ou éventuels de courtiers membres s'attendent à ce que leurs renseignements de nature délicate soient respectés et fassent l'objet d'une protection suffisante et pertinente. En outre, certaines obligations juridiques sont imposées aux courtiers membres de l'OCRCVM au chapitre de la protection des renseignements personnels.

le nombre d'incidents de sécurité imputés aux partenaires et aux fournisseurs ne cesse d'augmenter d'année en année. Les organisations devraient gérer les expositions au risque de cybersécurité qui découlent de ces relations en exerçant une fonction rigoureuse de diligence raisonnable et en établissant des politiques de vérification et de rendement précises.

Le présent guide de pratiques exemplaires en matière de cybersécurité expose des pratiques courantes et des suggestions qui peuvent ne pas s'appliquer ou ne pas être pertinentes dans certains cas. Ce guide n'a pas pour objet de présenter une norme minimale ou maximale de ce qui constitue un ensemble de pratiques appropriées en matière de cybersécurité pour les courtiers membres de l'OCRCVM. La gestion efficace des cyberrisques consiste notamment à analyser la situation qui est propre à chaque courtier.

Ce guide ne crée aucune nouvelle obligation légale ni ne modifie des obligations déjà imposées, et il ne vise nullement à le faire. L'information qu'il renferme est fournie uniquement à titre indicatif et nous ne pouvons pas garantir qu'elle est complète et exacte. Cette information ne doit pas être considérée non plus comme un avis juridique ou professionnel. Les courtiers membres qui désirent obtenir d'autres orientations devraient consulter un professionnel en cybersécurité pour obtenir des conseils précis sur leur programme de cybersécurité.

Objet et applicabilité

La présente publication a pour objet de bien faire comprendre les contrôles de sécurité spécifiques axés sur des normes qui composent un programme de pratiques exemplaires en matière de cybersécurité.

La mise en œuvre des contrôles devrait varier entre les divers courtiers membres, selon les menaces, les vulnérabilités et la tolérance au risque qui sont propres à chacun. Les membres du secteur des valeurs mobilières peuvent déterminer les activités qui sont importantes pour la prestation de services essentiels et ils peuvent établir l'ordre de priorité entre les investissements de manière à optimiser le rendement de chaque dollar dépensé.

Le présent guide comporte les objectifs précis suivants :

- Établir et tenir à jour un vigoureux programme de sensibilisation à la cybersécurité qui est bien appliqué, et veiller à ce que les utilisateurs soient conscients de l'importance de bien protéger les renseignements de nature délicate et les risques d'un mauvais traitement de l'information;[2]

- Faciliter une démarche uniforme et comparable pour le choix et la spécification des contrôles de sécurité des systèmes informatiques des courtiers membres;[i]

[2] La sensibilisation à la cybersécurité est un élément essentiel d'un programme étoffé de cybersécurité. Nous traiterons cette question plus en détail dans les prochaines sections, mais fondamentalement, la sensibilisation à la cybersécurité exige des politiques et une formation sur le sujet (p. ex., une politique de poste de travail ordonné pour éviter des atteintes à la sécurité par le personnel chargé des installations, comme les concierges ou les agents de sécurité, et une formation annuelle obligatoire pour tous les employés).

- Fournir un catalogue de contrôles de sécurité pour satisfaire les besoins actuels de protection de l'information et les exigences relatives aux besoins futurs selon l'évolution des menaces, des exigences[3] et des technologies;

- Jeter des bases en vue de l'élaboration des méthodes et procédures d'évaluation interne pour déterminer l'efficacité des contrôles de sécurité.

Ce cadre de pratiques exemplaires se veut un document vivant et il continuera d'être mis à jour et amélioré à mesure que le secteur commentera sa mise en œuvre. Les leçons tirées de la première livraison de ce cadre aux courtiers membres seront intégrées aux versions futures. Ainsi, le document continuera de satisfaire les besoins des courtiers membres dans un contexte de menaces dynamiques et de solutions novatrices.

[3] Quelques-unes de ces catégories de protection des renseignements (p. ex., l'exposition ou la perte de renseignements importants sur la clientèle) comportent des exigences spéciales plus restrictives en matière de réglementation pour la protection de la sécurité de l'information. Si ces renseignements ne sont pas correctement protégés, il pourrait en découler l'imposition de fortes amendes et pénalités par les organismes de réglementation des États-Unis et du Canada.

Public cible

Le présent guide s'applique aux courtiers membres de l'OCRCVM, sans égard à leur taille et à leurs budgets, mais il s'adresse tout particulièrement aux sociétés de petite et moyenne taille.

Sa structure facilite la communication des activités de cybersécurité et de leurs résultats dans l'ensemble de l'entreprise d'un courtier membre – depuis les échelons opérationnels et de mise en œuvre jusqu'à la haute direction. Il s'adresse à un auditoire diversifié, notamment les membres de la haute direction, les auditeurs, les utilisateurs, les professionnels de la sécurité de l'information, les responsables de la technologie de l'information et le personnel sur le terrain.

Parmi les membres du personnel susceptibles de profiter de l'examen des contrôles de sécurité énoncés dans le présent document, mentionnons :

- les personnes qui ont accès aux systèmes, notamment les **utilisateurs**;
- les personnes qui exercent des **fonctions liées aux systèmes d'information, à la sécurité et/ou à la gestion et à la surveillance des risques** (p. ex., les chefs de l'informatique, les responsables de la sécurité de l'information, les gestionnaires des systèmes d'information, les gestionnaires de la sécurité de l'information);
- les personnes qui exercent des **fonctions liés à l'élaboration de systèmes d'information** (p. ex., les gestionnaires de programme, les concepteurs et les développeurs de systèmes, les spécialistes de la sécurité de l'information et les intégrateurs de systèmes);
- les personnes qui exercent des **fonctions liées aux activités et à la mise en œuvre de la sécurité de l'information** (p. ex., les responsables de missions et d'entreprises, les responsables de systèmes d'information, les fournisseurs de contrôles communs, les propriétaires de l'information et responsables de la gérance de l'information, les administrateurs de système, les chefs de la sécurité des systèmes d'information);
- les personnes qui exercent des **fonctions liées à la surveillance et à l'évaluation de la sécurité de l'information** (p. ex., les auditeurs, les évaluateurs de systèmes, les évaluateurs, les vérificateurs/validateurs indépendants, les analystes, les responsables de systèmes d'information).

1 Contexte

1.1 Définition de la cybersécurité

Il existe actuellement de nombreuses définitions acceptées de la cybersécurité :

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

Fondamentalement, la cybersécurité a pour but de protéger votre entreprise contre ceux qui souhaitent lui nuire, voler vos renseignements ou votre argent, ou utiliser vos systèmes pour cibler vos pairs sur le marché.

La cybersécurité n'est pas difficile, elle est simplement complexe. L'Australian Signals Directorate (ASD) a groupé les 35 plus importantes stratégies nécessaires pour protéger les réseaux informatiques.[ii] Parmi celles-ci, l'ASD précise que la mise en œuvre des quatre principales stratégies de cybersécurité permettra d'atténuer au moins 85 % des cyberintrusions ciblées. Ces quatre principaux contrôles sont les suivants :

1. L'établissement d'une liste blanche des applications – ne permettre, sur les réseaux, que les applications qui ont été autorisées.
2. La correction de la sécurité des applications – mettre en œuvre des pratiques efficaces pour déployer rapidement de nouveaux correctifs de sécurité.
3. La correction de la sécurité des systèmes d'exploitation – même pratique que la précédente, mais elle porte sur les systèmes d'exploitation.
4. La limitation des privilèges administratifs – n'autoriser que le personnel digne de confiance à configurer, à gérer et à surveiller les systèmes informatiques.

Le défi consiste à exécuter ces tâches et d'autres fonctions connexes d'une manière complète et globale tout en facilitant les fonctions opérationnelles essentielles d'une entreprise prospère.

Le présent document facilite cet effort en fournissant un guide consultable aux professionnels de la sécurité, aux membres de la haute direction d'une entreprise et aux employés des courtiers membres de l'OCRCVM, pour leur permettre de comprendre la menace de cybersécurité qui pèse sur leur entreprise, et d'élaborer un programme efficace de protection contre les cybermenaces.

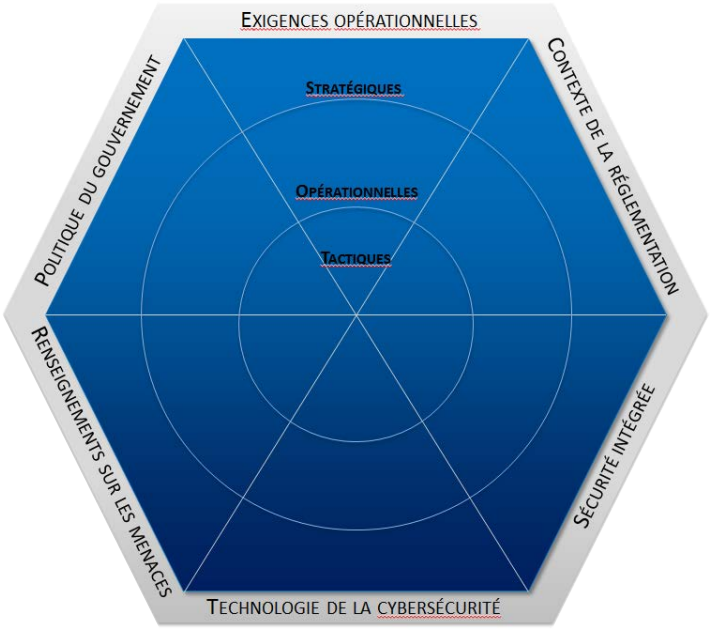


Figure 1 – Cadre conceptuel de la cybersécurité

La cybersécurité ne représente pas un problème portant uniquement sur la TI, il s'agit d'un problème d'entreprise qui exige une approche interdisciplinaire et un vaste engagement en matière de gouvernance pour faire en sorte que tous les volets de l'entreprise soient bien alignés pour appuyer des pratiques efficaces de cybersécurité.

La Figure 1 propose un cadre conceptuel qui permet de comprendre tous les aspects de la cybersécurité, ce qui comprend des discussions, des solutions et des services.

- Le secteur est guidé par *les politiques du gouvernement* qui donnent vie aux cyberdéfenses, et par le *Contexte de la réglementation* qui établit des normes de conduite.
- Les *Exigences opérationnelles* précisent les éléments spécifiques de la cybersécurité qui sont nécessaires pour atteindre les objectifs de l'entreprise.
- Les *Renseignements sur les menaces* recueillis dans les journaux, auprès des gouvernements, des partenaires du secteur, des fournisseurs du milieu de la sécurité,

et dans le cadre d'initiatives internes, établissent le contexte auquel les mesures de sécurité doivent permettre de faire front, maintenant et à l'avenir.

- Les activités de *Sécurité intégrée* qui se rapportent à la cybersécurité, à la sécurité physique et à la sécurité du personnel fournissent collectivement les éléments intégrés d'une solution de protection efficace.
- Enfin, la *Technologie de la cybersécurité* sous-tend mais ne dirige pas une politique efficace de cybersécurité. La technologie est trop souvent perçue comme la solution et non comme un simple élément d'une plus vaste stratégie.

Une vaste approche qui groupe ces six éléments dans une stratégie adaptable de cybersécurité encadrera les grandes priorités et orientera les mesures à prendre pour atténuer les cyberrisques qui menacent les actifs, les systèmes et l'information.

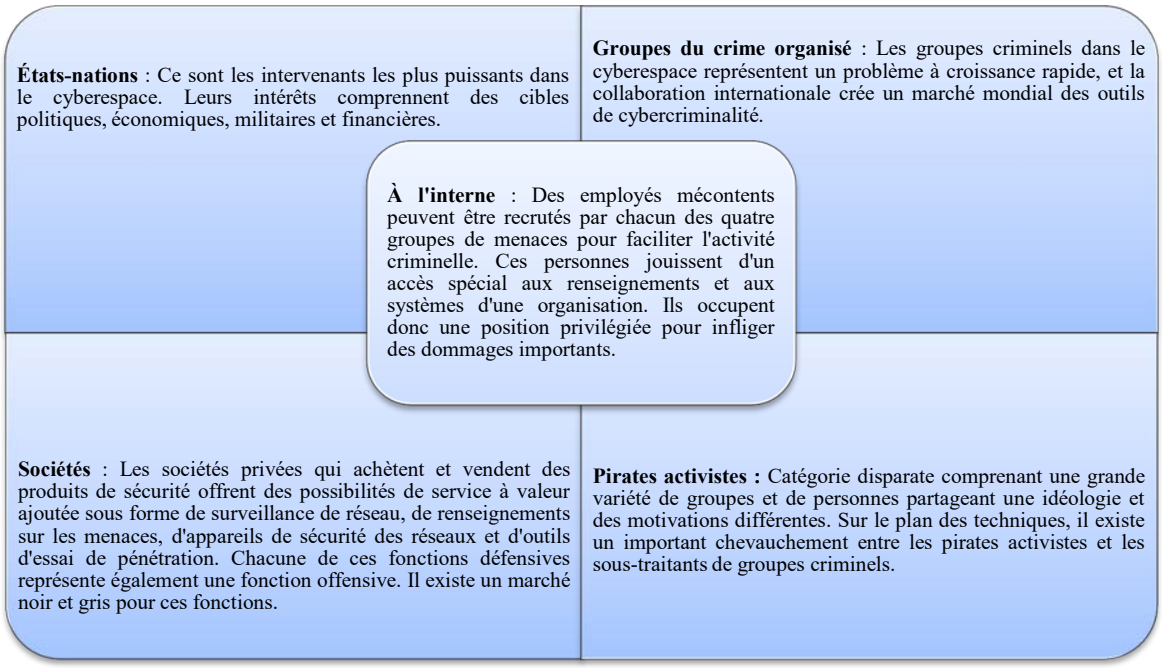
Le présent document a pour objectif de mettre à la disposition des membres de l'OCRCVM les outils dont ils ont besoin pour concevoir et mettre en œuvre des programmes efficaces de cybersécurité.

1.2 Contexte des menaces

Le secteur des valeurs mobilières est confronté à diverses menaces de cybersécurité qui évoluent rapidement, notamment des pirates qui infiltrent des systèmes, des initiés qui compromettent les données de l'entreprise ou de ses clients pour en tirer un gain commercial, les États-nations qui peuvent acquérir des renseignements pour faire progresser des objectifs nationaux, et des pirates activistes qui peuvent avoir pour objectif de déstabiliser une organisation et de la mettre dans l'embarras.

Selon l'environnement dans lequel se trouve un système d'information ou un réseau, et selon le type de renseignements que celui-ci doit permettre de soutenir, des menaces de catégories diverses cibleront divers types de renseignements ou d'accès.

Parmi les menaces les plus importantes et les plus problématiques, mentionnons les attaques complexes prenant la forme de menaces persistantes avancées (MPA), dont l'activité est en grande partie appuyée, directement ou indirectement, par un État-nation. Les MPA ciblent avec soin des données de grande valeur dans chaque secteur, de l'aérospatiale au commerce de gros, et de l'éducation aux finances.



Les sondages sur la cybersécurité menés par la FINRA en 2011 et 2014 ont permis de dégager les **trois menaces principales dans le secteur des valeurs mobilières,** à savoir :

- les pirates qui infiltrent les systèmes d'entreprise;
- les employés qui compromettent les données de l'entreprise ou de ses clients;
- les risques opérationnels.

Les entreprises doivent connaître les menaces qui sont à la fois les plus probables et les plus dangereuses pour leur situation particulière afin d'élaborer et de mettre en œuvre efficacement leur stratégie de cybersécurité.

Fraude par courriel [xxxii]

Un type de fraude télégraphique qui vise actuellement les entreprises prend la forme d'escroquerie au chef d'entreprise (ECE), qui constitue un type d'hameçonnage. La victime éventuelle reçoit un courriel qui semble provenir du service des ressources humaines ou des services techniques de son employeur. Les fraudeurs créent des adresses courriel qui reprennent fidèlement celles des services réels. Un message par courriel est envoyé au service de la comptabilité pour aviser que le « patron » travaille hors du bureau et a repéré un paiement en souffrance qui doit être effectué dès que possible. Le « patron » demande l'exécution du paiement et fournit le nom d'une banque et un numéro de compte bancaire dans lequel les fonds, habituellement d'un montant élevé, doivent être déposés. Les pertes dépassent généralement 100 000 $.

Étude de cas – Fraude par courriel – Février 2015

La chef des finances d'Infront Consulting Group Inc., société installée à Toronto et à Las Vegas, a reçu un courriel semblant provenir du chef de la direction, qui lui demandait de « traiter un paiement de 169 705,00 $US ». Les instructions jointes à la demande du virement télégraphique précisaient que le paiement devait être adressé à une société de courtage en valeurs mobilières de Naples, en Floride.

Le plan a échoué seulement parce que, par coïncidence, le premier dirigeant d'Infront a téléphoné à la chef des finances au moment où elle examinait la requête. Lorsqu'elle a demandé à quelles fins l'argent serait utilisé, le premier dirigeant lui a déclaré qu'il ne savait rien de cette requête. Un examen plus approfondi a révélé que le courriel avait été envoyé à partir d'une adresse semblable à celle de la société, mais que seule la lettre « I » manquait dans le terme « Consulting ».

2 Introduction

2.1 Objet et applicabilité

Un cadre de cybersécurité est constitué d'un ensemble d'activités de cybersécurité, de résultats souhaités et de renvois applicables qui sont communs à l'ensemble des secteurs clés de l'infrastructure. Ces cadres peuvent présenter les normes, les lignes directrices et les pratiques du secteur d'une manière qui permet la communication des activités de cybersécurité et leurs résultats à tous les courtiers membres – depuis la haute direction jusqu'aux échelons opérationnels et de mise en œuvre.

Le Cadre de cybersécurité du NIST se compose de cinq fonctions simultanées et continues : Identifier, Protéger, Détecter, Intervenir, Recouvrer. Ensemble, ces fonctions fournissent un point de vue stratégique de haut niveau portant sur le cycle de vie de la gestion du risque de cybersécurité d'une organisation. Ce cadre souligne les principales catégories et sous-catégories sous-jacentes de chacune des fonctions. Il ajoute à chaque sous-catégorie un index présentant des exemples de références informatives, notamment les normes, lignes directrices et pratiques existantes.

2.2 Synthèse du document

2.2.1 Lien avec d'autres publications portant sur le contrôle de la sécurité

Le présent document repose sur diverses sources – notamment les contrôles de sécurité employés dans les domaines de la défense, de l'audit et des finances, les contrôles effectués dans différents secteurs d'activité ou contrôles de processus, et les contrôles employé dans le domaine du renseignement de sécurité – ainsi que sur divers contrôles définis par des organismes de normalisation nationaux et internationaux. Les lignes directrices ont été élaborées d'un point de vue technique pour créer un ensemble de contrôles de sécurité stables et largement applicables aux systèmes informatiques et aux courtiers membres.

Les documents, principes et pratiques exemplaires qui suivent constituent le fonds documentaire :

1. SANS – Les 20 principaux contrôles de sécurité essentiels de SANS
   - Ensemble recommandé de mesures pour la cyberdéfense qui propose des façons précises et pratiques de contrecarrer les attaques les plus envahissantes.
2. Small Business Information Security: The Fundamentals (NISTIR 7621)
   - Énonce les mesures *absolument nécessaires* que doit prendre une petite entreprise pour protéger ses renseignements, ses systèmes et ses réseaux.
3. NIST – Cybersecurity Fundamentals For Small Business Owners
   - Pratiques exemplaires recommandées par le National Institute of Standards and Technology pour aider les petites entreprises à protéger la sécurité des renseignements de leurs clients et de leurs employés.

4. Security and Privacy Controls for Federal Information Systems and Organizations (NIST 800-53r4)
   - La norme internationale des contrôles de sécurité couvrant 17 domaines, notamment le contrôle de l'accès, l'intervention en cas d'incident, la continuité des activités, et la reprise après sinistre.
5. Plan de gestion des incidents de la TI du gouvernement du Canada
   - Porte sur les menaces, les vulnérabilités et les incidents de cybersécurité qui influent sur le service aux Canadiens, sur les activités du gouvernement, sur la sécurité ou la protection des renseignements personnels, ou sur la confiance envers le gouvernement.

2.2.2 Contrôles opérationnels, techniques et de gestion

Le catalogue des contrôles de sécurité énoncés dans le présent document peut être utilisé efficacement pour gérer le risque de sécurité de l'information à trois niveaux distincts – le niveau de l'organisation, le niveau de la mission/des processus opérationnels et le niveau des systèmes d'information.

Les organisations ont le devoir de sélectionner les contrôles de sécurité appropriés, de les appliquer correctement et d'en démontrer l'efficacité pour respecter les exigences établies en matière de sécurité. Le présent document a pour but de compléter les processus de gestion des risques de cybersécurité de l'organisation, mais non de les remplacer. Les utilisateurs qui appliquent des programmes de cybersécurité peuvent mettre à profit ce document pour déterminer les possibilités de les faire correspondre aux pratiques exemplaires du secteur, tandis que les courtiers membres qui ne disposent pas d'un programme de cybersécurité peuvent utiliser le document à titre de référence pour élaborer leur propre programme.

3 Pratiques exemplaires

3.1 Gouvernance et gestion des risques

La cybersécurité ne constitue pas uniquement un enjeu de TI. Il s'agit d'un défi à plusieurs volets qui exige une approche de gestion intégrée. La protection totale contre les cybermenaces est impossible. Par contre, une pratique exemplaire représente une approche axée sur les risques qui met en œuvre une vaste stratégie visant à éviter, à atténuer, à accepter ou à transférer délibérément les risques que posent les cybermenaces. Les sociétés doivent établir et tenir à jour un cadre approprié de gouvernance et de gestion des risques pour détecter et éliminer les risques auxquels sont exposés les réseaux et services de communication.

3.1.1 Cadre de gouvernance

La première mesure que doit prendre le conseil d'administration ou l'équipe de la direction consiste à déterminer les responsables au sein de la société qui doivent participer à l'élaboration d'un programme de cybersécurité. Parmi les principales mesures internes à prendre dans un premier temps, mentionnons la détermination des risques connus et des contrôles établis.

Une pratique exemplaire consiste à mettre sur pied un comité interorganisationnel composé de cadres supérieurs qui représentent l'éventail complet des connaissances et compétences de l'entreprise, entre autres la sécurité intégrée et la sécurité de la TI, de même que les responsables opérationnels.

Le leadership est un élément clé. La désignation d'un cadre de direction ayant de vastes responsabilités interfonctionnelles, comme le chef des finances ou le chef de l'exploitation, à la tête de ce comité, pourrait permettre de maintenir l'accent de cette initiative sur les préoccupations de l'ensemble de l'organisation, plutôt que de la cloisonner dans un réseau de renseignements sans les avantages d'une plus vaste adoption au sein de l'entreprise. Cette initiative devrait relever d'un comité spécial, notamment le comité d'audit ou le comité de gestion des risques ou, dans certains cas, du conseil d'administration.

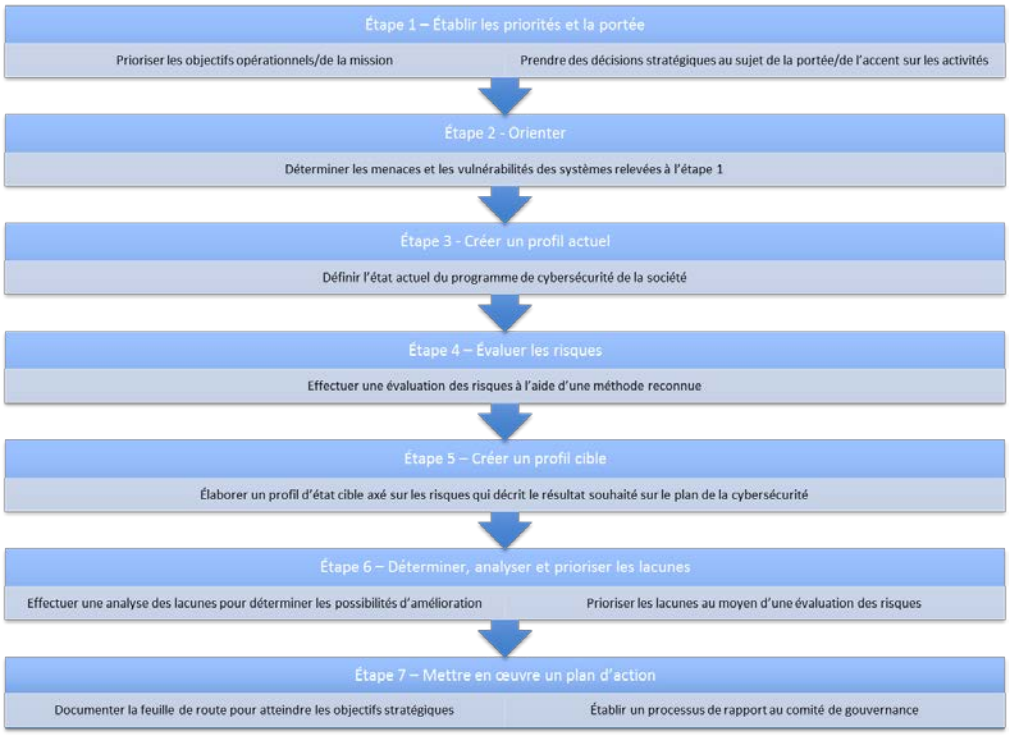


Figure 2 – Étapes de mise en œuvre du Cadre de cybersécurité

Le Cadre de cybersécurité du NIST prévoit un processus éprouvé qui permet d'élaborer et de gérer un programme de cybersécurité. La Figure 2 ci-dessus énonce les étapes que les conseils d'administration devraient exhorter les membres de la haute direction à mettre en œuvre. Ces derniers devraient aussi être tenus de faire rapport des progrès réalisés.

Une pratique exemplaire consiste à nommer un chef de la sécurité de l'information (CSI) et à lui attribuer des fonctions en matière de sécurité de l'information pour la supervision des initiatives de la société dans le domaine de la cybersécurité. Quelle que soit la personne nommée pour superviser ces initiatives, la cybersécurité est une charge partagée dans l'ensemble de la société, notamment avec les membres de la haute direction, le personnel, les experts-conseils,

les partenaires et les clients. La sensibilisation à la cybersécurité doit viser tous ces titulaires de charges.

Le programme doit débuter par la détermination des types de renseignements que détient la société et de leur localisation. Les renseignements sont souvent conservés dans plus d'un endroit à la fois, et différents contrôles sont mis en place pour en garantir la protection. Une approche axée sur les risques qui met l'accent sur les systèmes essentiels et ceux qui sont fondamentaux pour la mission permet de centrer les efforts sur les enjeux ayant le plus d'impact. Les sociétés devraient créer un relevé précis des éléments suivants :

- Les dispositifs et systèmes matériels
- Les plateformes logicielles et leurs applications
- Les cartes de ressources réseau, connexions et flux de données
- Les branchements aux réseaux de la société
- Une liste de priorités en matière de ressources, fondée sur la sensibilité et la valeur opérationnelle
- Les capacités et pratiques de branchement, évaluées au chapitre de la suffisance, de la conservation et de l'entretien sûr

L'initiative devrait être axée sur les « actifs attrayants » de la société et sur la priorisation des autres données et systèmes. Lorsque cette étape est franchie, la société peut passer à l'élaboration d'un programme de cybersécurité axé sur les risques qui accorde le niveau de protection le plus élevé aux données qui comportent la plus grande valeur. Elle devrait créer un profil à jour de ses protections de cybersécurité.

Les initiatives de cybersécurité devraient viser les menaces propres au secteur d'activité et aux sociétés se trouvant dans la même situation. Les sociétés devraient effectuer des évaluations des risques de menace propres aux systèmes prioritaires, dans le but de mieux comprendre les priorités en fonction des risques. Le contexte opérationnel doit être constamment examiné afin de déterminer la probabilité d'un événement de cybersécurité et de son incidence. Il s'agit d'un processus continu et répétitif reposant sur l'évolution du contexte de la TI au sein de la société, et sur l'évolution de son modèle opérationnel.

À partir de l'information recueillie au moyen de l'évaluation des risques, la société devrait déterminer le profil cible qui porte sur les résultats souhaités en matière de cybersécurité. Ce profil devrait dépasser les systèmes de la société et englober ceux des intervenants de l'extérieur sur lesquels il repose, afin d'inclure les entités, clients et partenaires commerciaux du secteur.

Une fois le profil cible établi, la société doit le comparer au profil actuel et déterminer les lacunes. Ces lacunes devraient être classées par ordre de priorité dans un plan énonçant les lacunes d'après des facteurs propres à la société, plus particulièrement les besoins opérationnels, la configuration des systèmes et les ressources disponibles pour combler les écarts. Chaque société est différente; par conséquent, l'élaboration d'un plan réalisable à l'aide de ressources suffisantes devrait constituer l'objectif.

La mise en œuvre du plan d'action et le suivi des progrès doivent devenir une fonction opérationnelle de base. Dans le contexte actuel, la cybersécurité n'est pas un projet ponctuel, mais plutôt une obligation continue pour la haute direction et le conseil d'administration – pour les sociétés de toutes tailles. La haute direction doit surveiller son plan de mise en œuvre et faire rapport périodiquement au conseil d'administration au sujet des progrès réalisés en vue de l'atteinte du résultat cible ultime. Même si le Cadre de cybersécurité du NIST prévoit un excellent ensemble d'outils pour orienter la mise en œuvre d'un programme de cybersécurité, chaque société doit déterminer les normes, lignes directrices et pratiques qui conviennent le mieux à ses besoins.

3.1.2 Participation du conseil d'administration et de la haute direction

La National Association of Corporate Directors (NACD) cite cinq principes de cybersécurité qui relèvent des conseils d'administration, à savoir :

Les administrateurs doivent comprendre la cybersécurité et l'envisager comme un enjeu de gestion des risques à la grandeur de l'organisation, et non comme une simple question de TI.

- Les conseils d'administration doivent reconnaître que la cybersécurité dépasse les réseaux de la société et englobent les fournisseurs, les partenaires, les sociétés affiliées et les clients.
- Il convient de comprendre l'écosystème dans son entier et de veiller à ce que le leadership de la direction en matière de sécurité soit de grande portée.

Les administrateurs doivent comprendre les répercussions juridiques des cyberrisques, compte tenu de la situation particulière de leur société.

- Les cyberattaques de haut niveau ont entraîné une vaste gamme de poursuites. Les conseils d'administration doivent comprendre la teneur de la responsabilité et se protéger adéquatement contre ces menaces.
- Les administrateurs devraient demander à la direction d'obtenir le point de vue de leur avocat externe au sujet de la divulgation éventuelle en cas d'infraction à la sécurité, et l'intégrer à leurs plans d'action.

Les conseils d'administration devraient avoir un accès suffisant à l'expertise en cybersécurité, et les discussions au sujet de la gestion des cyberrisques devraient avoir lieu périodiquement et occuper une période suffisante à l'ordre du jour des réunions du conseil.

- Les administrateurs devraient demander périodiquement conseil au sujet de la cybersécurité et tenir des séances d'information approfondies à l'interne et avec des experts de l'extérieur, entre autres des cabinets spécialisés en cybersécurité, des organismes gouvernementaux, des associations sectorielles et des institutions homologues.

Les administrateurs devraient fixer une attente selon laquelle la direction établira un cadre intégré de gestion des cyberrisques doté de ressources humaines et budgétaires suffisantes.

- Les administrateurs devraient veiller à ce que la cybersécurité soit une fonction intersectorielle dirigée par un cadre supérieur investi d'un pouvoir intersectoriel, notamment le chef des finances ou le chef de l'exploitation.
- Les administrateurs devraient s'attendre à recevoir de la direction des rapports périodiques renfermant des mesures qui quantifient les répercussions des initiatives de gestion des risques issus des cybermenaces déclarées sur les activités de la société.
- Les administrateurs devraient veiller à ce qu'un budget précis de cybersécurité soit lié à la stratégie d'exécution, de sorte que le programme ne soit pas exclusivement raccordé à un secteur.

La discussion des cyberrisques au conseil d'administration et au sein de la direction devrait préciser les risques à éviter, à accepter, à atténuer ou à transférer au moyen d'une assurance, et prévoir des plans précis pour chaque approche envisagée.

- La cybersécurité totale est un objectif irréaliste; la concentration des ressources autour des données les plus essentielles constitue une pratique exemplaire.
- Les administrateurs devraient faire en sorte que leur société adopte une stratégie précise comportant des approches superposées qui répondent le mieux aux besoins opérationnels de la société.

La surveillance de la mise en œuvre du vaste programme de cybersécurité décrit précédemment incombe à tous les conseils d'administration, quelle que soit la taille de la société.

Étude de cas – Ashley Madison – Juillet 2015 [xxxiii]

La société canadienne Ashley Madison a été la cible de pirates en juillet 2015. Se désignant l'Impact Team, les pirates s'opposaient au modèle d'entreprise de la société qui offrait une tribune facilitant l'infidélité conjugale de personnes mariées. L'objectif des pirates consistait à obliger la société à mettre un terme à ses activités, sans quoi ils menaçaient de diffuser les données volées.

En août 2015, les pirates ont divulgué les profils de quelque 39 millions de clients, y compris leur profil d'utilisateur, leurs noms et leurs adresses courriel. Les avocats représentant les victimes canadiennes ont intenté un recours collectif d'un montant de 760 millions de dollars en dommages-intérêts. La société-mère, Avid Life Media, a reporté à une date indéterminée l'imminent premier appel public à l'épargne aux termes duquel elle espérait obtenir une somme de 200 millions de dollars.

3.2 Pratiques exemplaires recommandées : petites et moyennes sociétés membres

La cybersécurité est une responsabilité partagée – les personnes, les processus, les outils et les technologies travaillent ensemble pour protéger les biens d'une organisation.

La protection des biens de votre organisation exige l'atteinte de **trois objectifs fondamentaux** :[iii]

- **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 détiennent l'autorisation de les consulter.
- **Intégrité**
  Maintenir l'intégrité des renseignements pour qu'ils demeurent complets, intacts et non corrompus.
- **Disponibilité**
  Garantir la disponibilité des systèmes, des services et des renseignements au moment où l'entreprise ou ses clients en ont besoin.

Ces objectifs peuvent être atteints en exécutant les fonctions du Cadre de cybersécurité énoncées ci-après :[iv]

1. Préciser les renseignements qui doivent être protégés, de même que toutes les menaces et les risques qui y sont rattachés.
2. Protéger les biens à l'aide de mesures de protection convenables.
3. Détecter les intrusions, les infractions à la sécurité et l'accès non autorisé.
4. Intervenir en cas d'événement de cybersécurité potentiel.
5. Se remettre d'un événement de cybersécurité en rétablissant les activités et services normaux.

3.3 Enquête de sécurité sur le personnel et menaces internes

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

Un sondage mené en 2012 par un fournisseur de services de cybersécurité, Cyber-Ark, a permis de constater que 71 % des 820 gestionnaires de TI et professionnels de niveau C participants estiment que les menaces internes constituent leur principale préoccupation en matière de cybersécurité.[v]

Par définition, une menace interne est personnifiée par [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 dépassé ou mal utilisé cet accès, et a ainsi porté atteinte à la confidentialité, à l'intégrité ou à la disponibilité des renseignements ou des systèmes informatiques du courtier membre. »[vi]

Certains des risques que posent les menaces internes dans le secteur financier sont énoncés ci-après :[vii]

- La divulgation non souhaitée de données confidentielles sur les clients et les comptes – qui mettent en péril les relations les plus précieuses de l'organisation
- La fraude
- La perte de propriété intellectuelle
- La désorganisation de l'infrastructure essentielle
- Des pertes monétaires
- Des répercussions sur le plan réglementaire
- La déstabilisation, la désorganisation et la destruction des cyberbiens d'une institution financière
- L'embarras et le risque d'atteinte aux relations publiques et à la réputation

Selon le Carnegie Mellon's CERT Insider Threat Center, les employés qui posent le plus grand risque de menace interne sont :

- 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 monnayer la vente de 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 ont pris part à l'implantation de la propriété intellectuelle et qui estiment en être les propriétaires. Ils s'approprient donc cette propriété lorsqu'ils quittent l'organisation

Voici des recommandations qui permettront d'éliminer la menace interne :[viii]

- **Mettre sur pied une équipe pluridisciplinaire**
  Dans la mesure du possible, les organisations doivent compter sur une équipe composée de professionnels des Ressources humaines, de la Sécurité et des Services juridiques qui créent des politiques, qui dirigent la formation et qui surveillent les employés à risque.
- **Enjeux organisationnels**
  Comprendre si votre organisation s'expose à un plus grand risque en raison de facteurs organisationnels inhérents. Votre société compte-elle des bureaux, des fournisseurs ou des sous-traitants à distance, dans des régions où les différences culturelles, politiques ou linguistiques pourraient engendrer des conflits?
- **Examiner les processus de filtrage de sécurité préalable à l'embauche**
  Les renseignements recueillis au cours du processus aideront les gestionnaires chargés de l'embauche à prendre des décisions éclairées et à atténuer le risque d'embaucher un employé « problème ».
- **Élaborer des politiques et des processus**
  Il s'agit ici d'une liste de contrôle des secteurs particuliers de politique et de pratique qui doivent être pris en compte dans les structures de gouvernance de base d'une organisation.
- **Activités de formation et d'éducation**
  Ces activités sont essentielles pour 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 y appliquer des mesures d'intervention**
- **Anticiper et gérer les situations négatives en milieu de travail**
- **Établir une distinction entre les fonctions et les privilèges minimum**

En reconnaissant les torts qui ont pu être causés par les employés en poste ou qui ont quitté, l'organisation peut atténuer les dommages susceptibles de découler de menaces internes.

Étude de cas – Fuite de données internes – Janvier 2014

Les données personnelles d'au moins 20 millions d'utilisateurs de carte de crédit et de carte bancaire en Corée du Sud ont été volées à trois émetteurs de cartes par un expert-conseil temporaire travaillant pour le Bureau de crédit de la Corée, une agence de notation du crédit personnel.

Les données volées ont été vendues à des sociétés de marketing par téléphone et elles comprenaient les noms de clients, les numéros de sécurité sociale, les numéros de téléphone, les numéros de carte de crédit et la date d'échéance.

À la suite du vol, des dizaines de cadres supérieurs ont remis leur démission, les organismes de réglementation ont ouvert des enquêtes au sujet des mesures de sécurité en place dans les sociétés en cause, qui ont été tenues responsables de la totalité des pertes financières touchant les clients victimes de stratagèmes se rapportant au vol des données.

3.4 Sécurité physique et environnementale

La sécurité physique des biens de TI constitue une première ligne de défense en cybersécurité. L'effet du vol d'un ordinateur portable ou d'un téléphone intelligent peut être tout aussi perturbateur pour une organisation qu'une cyberattaque. Par conséquent, les mesures de protection tels les mots de passe et le PINS doivent être complétées par 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 volontaires ou involontaires 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.

Voici des recommandations touchant la sécurité physique et environnementale :

- Les employés devraient appliquer le principe du « bureau propre », c'est-à-dire que les employés devraient ranger les documents renfermant des renseignements de nature délicate avant de quitter leur zone de travail. En outre, un bureau propre évite que les renseignements de nature délicate se retrouvent entre les mains de personnes qui ne sont pas autorisées par la loi à les consulter. Le personnel des services d'entretien et les agents de sécurité font partie des employés qui n'ont pas « besoin de savoir ».
- N'autorisez les employés à avoir accès à votre zone de travail que s'ils ont un besoin opérationnel légitime.
- Limitez l'accès au contenu de votre ordinateur en verrouillant l'écran lorsque vous vous absentez de votre poste de travail.
- Protégez votre système d'information contre les variations de l'alimentation électrique ou les pannes de courant, et assurez-vous que votre ordinateur est branché dans un système d'alimentation sans coupure.
- Effectuez périodiquement des copies de vos renseignements pour être à l'abri des sinistres, tel un incendie ou une inondation.
- Les organisations de petite et moyenne taille doivent mettre en place un plan d'intervention portant sur les problèmes de sécurité physique. L'ampleur des contrôles de sécurité physique mis en œuvre doit être proportionnelle au niveau de sensibilité des renseignements protégés.

3.5 Sensibilisation à la cybersécurité et formation

Le risque de cyberattaque contre des institutions financières ne cesse de croître, à mesure que le 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 leurs intervenants, elles demeurent constamment la cible de cybercriminels souhaitant voler leur propriété intellectuelle et leurs renseignements confidentiels. Dans son *Global State of Information Security® Survey,* publié en 2015, Price Waterhouse Coopers laisse à entendre que les entreprises qui appliquent un programme de sensibilisation à la sécurité déclarent des pertes financières moyennes sensiblement moins élevées à l'égard des incidents de cybersécurité. Le cabinet souligne également qu'un programme efficace de sensibilisation à la sécurité exige un des fonds suffisants.[ix]

Bon nombre d'organisations investissent massivement dans les contrôles techniques pour protéger leurs systèmes informatiques et leurs données. Toutefois, la plupart de ces contrôles deviennent inutiles parce que les employés n'ont pas été sensibilisés à la cybersécurité ou n'ont pas reçu de formation en la matière. Les employés prennent des risques en ligne, ce qui accroît de beaucoup les risques de cybersécurité auxquels s'expose leur organisation. Les activités risquées des employés comprennent l'ouverture de courriels douteux et la non-protection de renseignements de nature délicate stockés sur leurs ordinateurs ou envoyés à partir de leurs ordinateurs. Le sondage *2015 Cyberthreat Defense Report Survey* révèle qu'une faible sensibilisation à la sécurité au sein du personnel demeure le plus important facteur nuisant à une défense efficace contre les cybermenaces.[x]

On a demandé aux participants au sondage de coter les problèmes qui nuisent à une défense efficace contre les cybermenaces.

Sur une échelle de 1 à 5 (5 représentant la note la plus élevée), dans quelle mesure chacun des problèmes qui suivent empêche-t-il votre organisation de se défendre efficacement contre les cybermenaces?

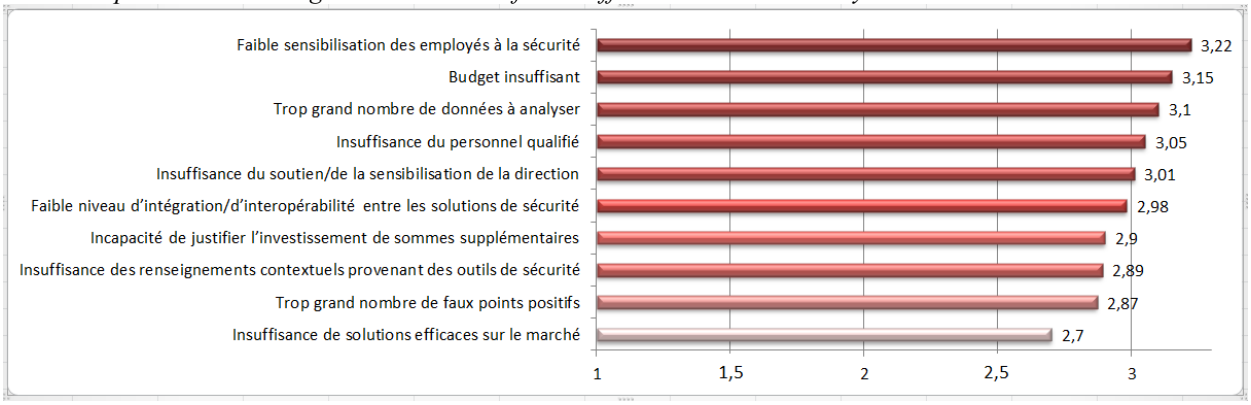


Figure 3 – Facteurs empêchant l'établissement de mesures de défense efficaces contre les cybermenaces (Source : 2015 Cyberthreat Defense Report*)*

Une faible sensibilisation à la sécurité trône au premier rang. Ce résultat souligne l'importance de la sensibilisation à la sécurité et de la formation en la matière comme principale activité qu'une organisation peut appliquer pour mieux se défendre contre les cyberattaques. Les employés devraient être informés des saines pratiques de cybersécurité et bien comprendre

qu'ils jouent un rôle crucial dans la protection des actifs informationnels de leur organisation. Grâce à une formation adéquate, les employés deviennent la première ligne de défense contre les cybermenaces.

Voici des recommandations touchant la sensibilisation et la formation :

- Mettre en œuvre des politiques portant sur l'utilisation sûre et acceptable des systèmes informatiques.
- Rendre obligatoire la formation et la sensibilisation à la cybersécurité pour tout le personnel. La formation peut se dérouler en classe, en ligne ou en séance vidéo, et elle doit 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 bien leur rôle et leurs responsabilités au chapitre de la cybersécurité.
- Les utilisateurs devraient être avisés de ne pas ouvrir de courriels douteux ni de cliquer sur des liens douteux, quelle qu'en soit la source.
- Les utilisateurs devraient être avisés de ne pas brancher des dispositifs au réseau, à moins d'avoir un motif professionnel légitime de le faire ou d'utiliser des dispositifs approuvés.
- Les utilisateurs devraient être avisés d'appliquer de saines pratiques en matière de mot de passe.
- Les utilisateurs devraient comprendre les dangers et les usages sûrs de médias externes (clés USB et DC).
- Les utilisateurs ne devraient pas télécharger ou installer des applications non autorisées parce leur contenu peut être malveillant.
- Les utilisateurs devraient comprendre que des sanctions seront imposées aux membres du personnel qui ne se conforment pas aux principes de sensibilisation à la cybersécurité et aux politiques de sécurité.
- Les méthodes de formation continue pour les cadres de direction peuvent comprendre des séances vidéo ou des webinaires qui ont pour but de sensibiliser les utilisateurs et de partager des renseignements visés par mandat.

Étude de cas – Rançongiciel – Juin 2015

Mahone Bay et Bridgewater, deux petites localités de la Nouvelle-Écosse, ont déclaré que les ordinateurs municipaux ont été infectés en juin 2015. Le virus connu sous l'appellation CryptoWall 3.0 a attaqué les répertoires non raccordés à un réseau, que ce soit au moyen d'un courriel d'hameçonnage envoyé à l'utilisateur d'un système, ou d'un site Web infecté visité par un employé de la localité. Lorsqu'un clic a été effectué sur le lien, les systèmes ont été infectés par le virus CryptoWall 3.0 et un deuxième virus, nommé CryptoLocker, a chiffré les fichiers du système ciblé. Une fois activés, les virus ont livré un message automatisé à l'utilisateur pour lui réclamer le paiement d'environ 900 $ pour le déverrouillage des fichiers infectés – il est presque impossible de déchiffrer les fichiers sans payer la rançon exigée. Le virus serait parvenu de groupes criminels de Russie.

Le recours aux techniques CryptoLocker est très répandu. Selon le département américain de la Justice, les attaques de ce virus ont infecté plus de 234 000 ordinateurs – ce qui a entraîné le paiement de rançons de 27 millions de dollars – au cours des deux premiers mois.

3.6 L'évaluation des menaces et des vulnérabilités

Les cybercriminels continuent de tirer profit des vulnérabilités de base des systèmes informatiques, notamment les systèmes d'exploitation Windows non corrigés, un mot de passe faible et une formation inadéquate des utilisateurs. Les organisations qui n'effectuent pas d'analyse des vulnérabilités et qui ne corrigent pas efficacement les faiblesses de leurs systèmes d'information s'exposent davantage à la compromission de leurs systèmes informatiques. Pour protéger leurs actifs informationnels contre la menace grandissante de cyberattaques qui ciblent les vulnérabilités des systèmes, davantage d'organisations ont inclus des évaluations de la vulnérabilité dans leurs programmes de cybersécurité. Ces évaluations permettent de déceler les vulnérabilités dans les systèmes informatiques. Les résultats de ces évaluations aident les organisations à localiser les risques de cybersécurité.[xi]

Voici des recommandations touchant 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 de priorité renfermant les vulnérabilités les plus pressantes 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.
- Veiller à ce que les outils d'évaluation de la vulnérabilité utilisés soient périodiquement mis à jour et renferment les renseignements les plus à jour sur les vulnérabilités.
- 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 faire passer au mode de production.

Services de réparation d'ordinateur non sollicités
Dans le cadre d'un tel stratagème, l'employé d'une société appelle une personne en se faisant passer, par exemple, pour le représentant de Microsoft; il informe l'interlocuteur que son ordinateur fonctionne au ralenti ou qu'il est touché par des virus. Il lui offre de réparer l'ordinateur sur Internet, ce qui nécessitera l'installation d'un logiciel, ou de procéder à distance sur son ordinateur avec son autorisation.

Dans des variantes récentes, le suspect s'est fait passer pour un représentant du Centre canadien de réponse aux incidents cybernétiques et il a adopté une approche plus directe. Il a indiqué à sa victime que son ordinateur était utilisé par des pirates et qu'elle pourrait en être tenue responsable si elle ne l'autorisait pas à réparer son ordinateur.

Autoriser un tiers à télécharger des logiciels ou à avoir accès à son ordinateur à distance comporte son lot de risques. Des enregistreurs de frappe ou d'autres logiciels malveillants pourraient être installés pour saisir des données de nature délicate, notamment les noms d'utilisateurs de services bancaires en ligne et des mots de passe, des renseignements sur les comptes bancaires, des renseignements d'identité, etc.

Étude de cas – Fraude à l'ingénierie sociale – Avril 2015

Mega Metals Inc., une entreprise qui transforme de la ferraille depuis 30 ans, a été victime de fraude en 2015 lorsque la sécurité du compte de courrier électronique utilisé par un courtier d'Italie a été compromise.

Mega Metals avait effectué un virement télégraphique de 100 000 $ à un fournisseur allemand en guise de paiement pour un conteneur de 40 000 livres de copeaux de titane. À la suite de l'opération, le fournisseur s'est plaint qu'il n'avait pas reçu le paiement. Une enquête a révélé qu'un logiciel malveillant implanté dans les systèmes informatiques d'un courtier avait permis à des criminels de saisir les mots de passe donnant accès à la boîte de courrier électronique du courtier et de falsifier les instructions de virement télégraphique pour un achat légitime.

3.7 Sécurité réseau

La connexion permanente d'une organisation à Internet l'expose à un milieu hostile de menaces qui évoluent de façon très rapide. En outre, les actions délibérées ou accidentelles des employés peuvent menacer le réseau.

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

- protéger le service de réseau;
- réduire la vulnérabilité des systèmes d'extrémité et des applications aux menaces provenant du réseau;
- protéger les données pendant leur transmission à travers le réseau.

Les cybercriminels sont constamment à la recherche de faiblesses dans les dispositifs de protection de réseaux exposés à Internet (p. ex., des pare-feu). Ces appareils protègent l'organisation contre les menaces émanant d'Internet. À défaut de pare-feu dans le périmètre du réseau pour protéger le réseau contre les menaces sur Internet, les cybercriminels pourraient facilement voler la propriété intellectuelle et des renseignements de nature délicate.

Une défense multicouche composée de pare-feu de la prochaine génération réduit sensiblement le nombre d'attaques Internet dans le réseau interne d'une organisation.

Voici des recommandations touchant la sécurité réseau :

- Acheter un pare-feu de la prochaine génération. Les petites entreprises peuvent se procurer ce type de pare-feu pour moins de 1 000 $. Ces pare-feu s'accompagnent des services de sécurité supplémentaires suivants :
  - Le filtrage des sites Web renfermant des éléments malveillants.
  - La protection contre les virus sur Internet et contre les programmes malveillants qui infiltrent le réseau.
  - La technologie de prévention des menaces qui examine le trafic réseau pour détecter et empêcher les vulnérabilités sur Internet d'infiltrer le réseau.
- Exiger l'authentification à double facteur pour tout accès à distance, notamment par RVP.
- Fractionner le réseau interne de l'organisation pour faire en sorte que les utilisateurs n'aient accès qu'aux services dont ils ont besoin à des fins professionnelles.
- Mettre en œuvre une solution de contrôle d'accès au réseau afin d'empêcher des systèmes informatiques inconnus de communiquer avec le réseau de l'organisation.
- Établir un comportement minimal normal pour les dispositifs réseau.

3.7.1 Sécurité des réseaux sans fil

Même si la connectivité sans fil offre l'avantage d'une mobilité et d'une productivité accrues, elle présente également un certain nombre de risques de sécurité fondamentaux. Dans bien des cas largement médiatisés, les vols de propriété intellectuelle et de renseignements de nature délicate ont été causés par des attaquants qui ont eu un accès sans fil aux organisations à l'extérieur de leurs locaux. Puisque les signaux sans fil sont habituellement émis à l'extérieur de l'infrastructure physique d'un immeuble, ils passent outre les mesures de protection du périmètre de sécurité filé, notamment les pare-feu et les systèmes de protection contre les intrusions.

Dans certains cas, les cybercriminels obtiennent un accès illimité au réseau interne d'une organisation en dissimulant des points d'accès sans fil non autorisés sur le réseau. Les employés mécontents ou d'autres membres du personnel ayant des intentions malveillantes, et prenant l'identité de membres du personnel d'entretien ou d'un agent de sécurité, sont habituellement responsables du placement de ces dispositifs. Il est extrêmement facile pour les cybercriminels d'utiliser les réseaux sans fil pour s'immiscer dans les organisations sans mettre les pieds dans leurs locaux. Il est donc essentiel de mettre en œuvre de vigoureuses mesures de protection de la sécurité pour atténuer ces risques.

Voici des recommandations touchant la sécurité des réseaux sans fil :

- Veiller à ce que chaque dispositif sans fil soit autorisé à être raccordé à un réseau en fonction d'un besoin professionnel légitime. Les organisations doivent refuser l'accès à tous les autres dispositifs sans fil, y compris les appareils Bluetooth.
- Effectuer une analyse de vulnérabilité des réseaux sans fil. Cette analyse permettra de déceler les vulnérabilités dans le réseau sans fil et de déterminer les dispositifs non autorisés sur le réseau.
- Déployer 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. La plupart des principaux fournisseurs de dispositifs sans fil vendent des solutions d'accès sans fil universel, des pare-feu et des SDISF destinés aux petites entreprises pour moins de 1 000 $.
- Désactiver l'accès sans fil sur les systèmes informatiques sans besoins professionnels légitimes. Afin de réduire la probabilité qu'un employé active à nouveau l'accès sans fil, il convient d'utiliser la configuration matérielle de l'ordinateur qui est accessible à l'amorce du système, puis de désactiver l'accès sans fil et d'exiger un mot de passe à quiconque tente de pénétrer dans la configuration matérielle de l'ordinateur
- À tout le moins, veiller à ce que la totalité du trafic dans le réseau sans fil soit protégée par chiffrement selon la norme Advanced Encryption Standard (AES) et la protection Wi-Fi Protected Access 2 (WPA2).
- À tout le moins, veiller à ce que les réseaux sans fil utilisent des protocoles d'authentification comme Extensible Authentication Protocol-Transport Layer Security (EAP/TLS).
- Désactiver les fonctions de réseau sans fil point à point des clients.
- Désactiver l'accès périphérique sans fil des dispositifs (notamment les appareils Bluetooth), à moins qu'il existe un besoin professionnel légitime.

Étude de cas – Réseau local sans fil compromis – Mai 2007

Des pirates ont volé 45 millions de dossiers de clients – notamment des millions de numéros de carte de crédit – de The TJX Companies Inc., en s'immisçant dans le réseau local sans fil de la clientèle de détail de cette société.

TJX avait protégé son réseau sans fil à l'aide du protocole Wired Equivalent Privacy (WEP) – l'une des formes de sécurité des réseaux locaux les plus faibles. Selon le Wall Street Journal, les pirates se sont introduits dans le protocole de chiffrement WEP utilisé pour transmettre des données d'appareils de vérification des prix, de caisses enregistreuses et d'ordinateurs dans un magasin du Minnesota. Les intrus ont ensuite recueilli des renseignements fournis par les employés qui se branchaient à la base de données centrale de la société, au Massachusetts, et ont volé des noms d'utilisateur et des mots de passe. À l'aide de ces renseignements, ils ont créé leurs comptes dans le système de TJX. Sur une période de 18 mois, leur logiciel a recueilli des données sur les opérations, notamment des numéros de carte de crédit, dans une centaines de gros fichiers.

Selon les analystes, l'infraction à la sécurité aurait coûté environ 1 milliard de dollars à la société, sans compter les frais de litige.

3.7.2 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 soit constamment géré et tenu à jour pour empêcher les utilisateurs non autorisés d'avoir accès au réseau de votre organisation.

Voici des recommandations touchant l'accès à distance protégé :[xiii]

- Mettre en œuvre une politique d'accès à distance et former le personnel pour qu'il la respecte.
- L'accès à distance ne doit être autorisé qu'à l'aide de technologies de RPV protégé.
- Configurer le RPV protégé de manière à interdire la tunnellisation partagée.
- Surveiller et consigner toutes les séances par accès à distance.
- Exiger l'authentification à double facteur pour toutes les séances par accès à distance.

3.7.2.1 Sécurité de l'accès à distance à point terminal

Les employés qui ont accès aux ressources de l'organisation à l'aide d'un RPV protégé devraient utiliser le matériel de la société. Outre les directives énoncées à la section Protection des systèmes d'information, les utilisateurs de l'accès à distance devraient appliquer les conseils suivants :[xiv]

- Veiller à ce que la solution de blocage de logiciels malveillants soit à jour de sorte qu'elle permette de surveiller en permanence l'activité malveillante.
- Ne pas transférer de renseignements vers des destinations non autorisées (p. ex., des dispositifs de stockage non autorisés, Hotmail, Gmail, DropBox).
- Ne pas brancher des dispositifs non autorisés dans les ordinateurs de la société (p. ex., des téléphones intelligents, des clés USB et des disques durs).
- Ne pas brancher des clés USB de la société sur des dispositifs non approuvés (p. ex., des ordinateurs portables, des ordinateurs personnels, des téléviseurs intelligents).
- Se méfier des appels téléphoniques, des visites et des courriels de personnes qui vous posent des questions sur les employés, leurs familles et des dossiers de travail de nature délicate.
- Ne pas répondre à des courriels douteux et ne pas cliquer sur des liens dans des courriels douteux.
- Ne pas laisser son ordinateur portable ou des appareils semblables dans un espace public, même un instant.
- Veiller à garder les renseignements confidentiels à son écran à l'abri du regard des curieux.
- Éviter les connexions inconnues, non familières et Wi-Fi gratuites, à moins qu'elles soient protégées par mot de passe et chiffrement.

Étude de cas – Piratage par accès à distance – Juin 2014

Les attaques au moyen d'outils à distance ont retenu l'attention depuis l'atteinte massive aux données des magasins Target en 2013; des pirates ont envahi les systèmes de point de vente de Target en utilisant un compte d'accès à distance appartenant à une entreprise de chauffage, ventilation et climatisation.

Plus récemment, les pirates ont infiltré les systèmes de paiement de plusieurs restaurants et entreprises de services alimentaires du Nord-Ouest des États-Unis en utilisant un compte d'accès à distance appartenant à un fournisseur de systèmes de point de vente. Dans cet incident, un compte LogMeIn utilisé par le fournisseur afin d'appuyer et de gérer à distance les réseaux de service à la clientèle a été corrompu, puis utilisé pour placer un logiciel de vol de données sur les systèmes de point de vente appartenant aux clients du fournisseur.

3.8 Protection des systèmes d'information

Bien qu'il soit essentiel de protéger le périmètre du réseau d'une organisation contre les menaces provenant d'Internet, il est tout aussi important que les systèmes soient eux-mêmes protégés contre les tentatives de piratage. De même, les ordinateurs de la société qui sont utilisés pour avoir accès aux ressources de l'entreprise à distance devraient être dotés des mêmes contrôles de sécurité que les ordinateurs sur place.

Voici des recommandations visant à protéger les systèmes d'information contre les menaces, tels les rançongiciels et les virus :

- Mettre en œuvre des processus de sauvegarde et de recouvrement et effectuer périodiquement des sauvegardes de vos systèmes.
- Déployer une solution de blocage de 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.
- Déployer une solution de blocage de 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 à des dispositifs internes, p. ex., des clés USB, aux personnes et groupes qui ont un besoin professionnel légitime.
- Utiliser des pare-feu personnels intégrés à Windows et des systèmes UNIX.
- Analyser tous les supports pour éliminer les programmes malveillants avant de les importer sur l'ordinateur de l'organisation.
- Installer toutes les mises à jour de sécurité des applications et des systèmes d'exploitation, notamment ceux offerts par la fonction intégrée de mise à jour de Windows.
- Surveiller l'utilisation et la tentative d'utilisation de dispositifs externes.
- Les utilisateurs à distance devraient recourir aux ressources d'accès de l'organisation à l'aide d'un RPV protégé et ils devraient être approuvés par authentification à double facteur.

Les fournisseurs, tels Norton et McAfee, vendent des solutions de sécurité terminales intégrées pour les systèmes informatiques personnels, de petites entreprises et de sociétés à coût très raisonnable.

3.8.1 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. Il s'agit d'une démarche qui permet aux employés d'apporter leur propre matériel (p. ex., leur ordinateur portable, leur téléphone intelligent et leur tablette) à leur lieu de travail et de l'utiliser pour avoir accès aux applications et aux données de l'organisation. Bien que cette politique présente de véritables avantages, elle comporte également d'importants risques. . Par exemple :

- L'employé peut perdre un appareil personnel qui renferme des renseignements de l'entreprise.
- L'employé peut accidentellement installer des applications de nature malveillante.
- L'employé peut accidentellement divulguer des renseignements de l'organisation, par exemple en autorisant des membres de sa famille ou des amis à utiliser un ordinateur portable renfermant des renseignements de nature délicate au sujet de l'entreprise.
- Il se peut que le concept AVEC entre en conflit avec des lois et règlements applicables du fait que son application incorrecte contrevienne aux lois et règlements sur le caractère privé des données.

Une entreprise devrait effectuer une vérification des risques et demander un avis juridique avant de décider si elle doit autoriser le concept AVEC et si elle peut gérer les risques qui y sont associés. Si elle décide d'adopter le concept, elle devrait mettre en œuvre une série de mesures d'atténuation des risques et des contrôles. Compte tenu du fait que l'application du concept AVEC en milieu de travail a donné lieu à de nombreux cas d'atteinte à la sécurité des données,[xv] il est important que les entreprises envisagent la possibilité d'appliquer une vaste politique fondée sur le concept AVEC. À tout le moins, cette politique devrait englober les éléments suivants :[xvi]

- À qui la politique s'applique-t-elle (p. ex., le personnel, les sous-traitants)?
- Quels appareils peuvent être utilisés (p. ex., des ordinateurs personnels, des tablettes)?
- À quels services ou renseignements donne-t-elle accès (p. ex., des courriels, des calendriers, des personnes-ressources)?
- Quelles sont les obligations de l'employeur et des membres du personnel (notamment les mesures de sécurité qui doivent être adoptées)?
- Quelles applications peuvent et ne peuvent pas être installées (p. ex., pour la navigation dans les médias sociaux, le partage, ou l'ouverture de fichiers)?
- Comment avoir accès aux applications et aux données?
    - Idéalement, les dispositifs non vérifiés devraient avoir accès à des applications et à des renseignements professionnels au moyen d'un ordinateur personnel virtuel. Citrix et VMware sont des exemples de sociétés offrant des produits d'ordinateur personnel virtuel qui conviennent bien à la mise en œuvre protégée du concept AVEC.
- Quelle aide et quel soutien le personnel de la TI peut-il offrir?
- Quelles sont les pénalités pour non-conformité (p. ex., la perte de privilèges liés au concept AVEC et autres procédures disciplinaires)?

3.8.2 Sauvegarde et récupération

Une organisation doit appliquer un plan de sauvegarde afin de se préparer en vue d'un sinistre, sinon elle risque de perdre sa propriété intellectuelle et des renseignements de nature délicate. Les sauvegardes garantissent que l'organisation pourra reprendre rapidement ses activités en rétablissant les fichiers perdus ou endommagés.

Les petites et moyennes entreprises ont accès aux options de sauvegarde suivantes :

- 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 branché au réseau. Un processus automatisé du serveur sauvegarde ensuite périodiquement les données sur les utilisateurs.

Voici des recommandations touchant la sauvegarde et la récupération :

- Mettre en œuvre un plan et amorcer la sauvegarde périodique des données.
- Pour atténuer le risque de vol/sinistre, conserver des copies des sauvegardes dans un endroit sûr à l'extérieur.
- Inclure les paramètres des systèmes et des logiciels dans vos sauvegardes.
- Tester périodiquement vos sauvegardes en versant vos fichiers dans un ordinateur d'essai pour vérifier le bon fonctionnement du processus de sauvegarde.

Étude de cas – Sauvegarde et récupération – Avril 2007

Un cabinet de comptables des États-Unis, A Desaur & Co., utilisait un système de récupération sur bande lorsqu'est survenue une panne de serveur en avril 2007. Le processus de récupération a complètement échoué parce que le fournisseur de service de soutien en TI n'avait pas effectué un essai des données récupérées, ce qui aurait pu permettre de constater que la sauvegarde n'avait pas été effectuée.

Après une récupération coûteuse et fastidieuse du disque dur, seulement 80 % des données ont pu être recouvrées, ce qui a entraîné la perte de précieuses données d'archive pour la société (préparation des comptes) et des travaux en cours (tenue de registres).

3.9 Gestion des comptes d'utilisateur et contrôle d'accès

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

Voici des recommandations touchant la gestion des comptes d'utilisateur et les contrôles d'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, notamment Microsoft Active Directory.
- Configurer les dispositifs de réseau et de sécurité pour utiliser le système centralisé d'authentification.
- Limiter le nombre de comptes à privilèges à ceux qui répondent à un besoin professionnel légitime.
- Contrôler l'accès aux journaux d'audit du système informatique.
- Examiner tous les comptes de système et désactiver les comptes qui ne peuvent être associés à un processus opérationnel et 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 à 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 de vérification si une enquête s'avère nécessaire, par exemple.
- Obliger les utilisateurs à se brancher à nouveau après une période fixe d'inactivité.
- Exiger que tous les comptes d'employés comportent des mots de passe forts, renfermant 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 les plus récents ne puissent pas être utilisés comme nouveau mot de passe.
- Exiger l'authentification à double facteur pour les comptes à privilèges ou les comptes donnant accès à des données ou à des systèmes de nature délicate. L'authentification à double facteur peut être activée à l'aide de cartes à puces assorties de certificats, de mots de passe à usage unique ou de facteurs biométriques.

Étude de cas – Comptes d'utilisateur compromis – Juillet 2015

Dans le cadre d'une lente cyberattaque lancée en Chine contre les réseaux du Bureau de la gestion du personnel des États-Unis, les auteurs ont obtenu l'accès réseau authentifié au réseau du Bureau en compromettant un compte d'utilisateur sans privilège du domaine Active Directory du Bureau appartenant à un sous-traitant KeyPoint.

Ils se sont servi de cet accès authentifié sans privilège pour obtenir la liste de tous les utilisateurs avec privilèges du déploiement Active Directory du Bureau, et ils ont ensuite suivi la liste de privilèges d'Active Directory (à l'aide de l'un de ces deux vecteurs d'attaque) pour compromettre un des comptes d'utilisateur avec privilèges pour avoir accès aux bases de données SF-86 et SF-85. Ils ont ensuite exfiltré les données.

3.10 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 d'identifier et de gérer tous les systèmes informatiques pour que seuls les systèmes autorisés aient 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 ou correctifs les plus récents ne sont généralement pas installés sur les systèmes et applications non autorisés, et parfois peu sûrs. Par conséquent, ces systèmes sont habituellement plus susceptibles d'être exploités.

Voici des recommandations touchant la gestion des actifs :

- Déployer et tenir à jour un outil automatisé de recherche des actifs, et l'utiliser pour mettre au point un relevé des systèmes branchés au réseau privé et public de l'organisation.
- Se brancher au serveur au moyen du Dynamic Host Configuration Protocol (DHCP) afin d'améliorer le relevé des actifs et détecter les systèmes inconnus à l'aide des renseignements fournis par le protocole.
- Veiller à ce que le système de relevé soit mis à jour lorsque de nouveaux appareils approuvés se raccordent au réseau.
- Déployer le Network Access Control (NAC) et l'authentification réseau à l'aide du protocole 802.1x. Ces services de sécurité empêchent des dispositifs non autorisés de se brancher au réseau.
- Utiliser les certificats des clients pour valider et authentifier les systèmes avant de les brancher à un réseau.

Étude de cas – Vulnérabilité d'applications/de programmes – Octobre 2014

Un groupe de pirates actifs à l'étranger ont creusé dans les systèmes informatiques de la banque JPMorgan Chase, compromettant les noms, adresses, numéros de téléphone et adresses courriel de 76 millions de ménages et de 7 millions de petites entreprises.

Les pirates ont obtenu une liste des applications et programmes exécutés sur les ordinateurs de la banque, qu'ils pouvaient contrevérifier à l'aide des vulnérabilités connues de chaque programme et application Web, à la recherche d'un point d'entrée dans les systèmes de la banque. Lorsque l'équipe de la sécurité de la banque a découvert l'attaque, les pirates avaient déjà obtenu le niveau de privilège administratif le plus élevé pour des dizaines de serveurs de la banque.

Par la suite, la banque a dû informer ses organismes de réglementation de la portée de l'attaque, remplacer ses programmes et applications et renégocier les ententes de licence avec ses fournisseurs de technologie.

3.11 Intervention en cas d'incident

La planification et la préparation en vue d'un incident de cybersécurité représente 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 la disponibilité 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 plusieurs sources, notamment les membres du personnel agissant dans un dessein malveillant, les membres du personnel dignes de confiance dont les actes causent des dommages par faute, et les cybercriminels qui lancent des attaques.

La complexité des programmes malveillants et des techniques appliquées par les cybercriminels continue de croître rapidement et, par conséquent, les incidents de cybersécurité sont de plus en plus courants. Les organisations doivent mener un dur combat aux cybercriminels qui, avec le temps et l'argent, peuvent détruire les mesures de protection les plus complexes. Les organisations doivent faire preuve de diligence raisonnable et prendre les mesures qui conviennent pour intervenir correctement en cas de cyberincident. Une intervention mal exécutée peut entraîner de lourdes pertes financières pour l'organisation, ruiner sa réputation et peut-être même la mener tout droit à la faillite.[xvii] Par conséquent, il est nécessaire d'élaborer et d'appliquer un plan d'intervention en cas d'incident afin de détecter rapidement les incidents, de limiter les pertes et la destruction, d'atténuer les faiblesses des systèmes d'information, et de garantir la reprise des activités après un incident de cybersécurité.

Suivent quelques objectifs de la gestion des incidents de cybersécurité :

- Neutraliser les incidents de cybersécurité avant qu'ils ne surviennent
- Limiter l'impact des incidents de cybersécurité sur la confidentialité, la disponibilité ou l'intégrité des services, des actifs informationnels et des activités du secteur des valeurs mobilières
- Atténuer les menaces et les vulnérabilités des incidents de cybersécurité
- Améliorer la coordination et la gestion des incidents de cybersécurité au sein du secteur des valeurs mobilières
- Réduire les coûts directs et indirects engendrés par les incidents de cybersécurité
- Faire rapport des constatations à la haute direction

Termes et expressions clés

Les définitions qui suivent reposent sur la Norme internationale de gestion des incidents de sécurité de l'information (ISO/IEC 27035).[xviii]

ÉVÉNEMENT DE CYBERSÉCURITÉ

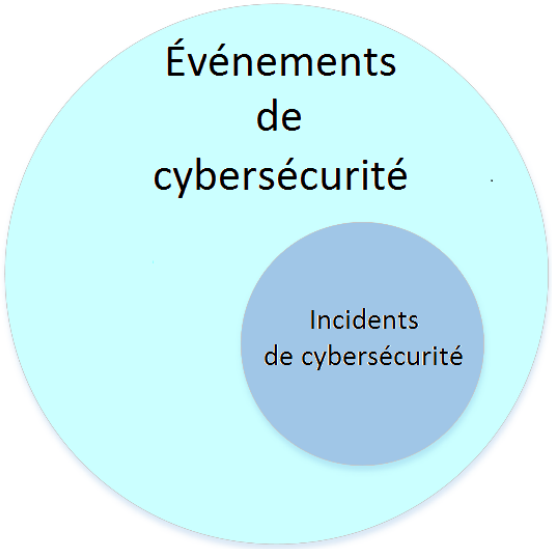
État d'un système, d'un service ou d'un réseau qui **indique une infraction possible** à la sécurité de l'information, une panne de contrôles ou une situation antérieure inconnue qui peut se rapporter à la sécurité.

INCIDENT DE CYBERSÉCURITÉ

Événement ou série d'événements non souhaités ou inattendus liés à la sécurité de l'information, qui sont **susceptibles de compromettre sensiblement les activités opérationnelles** et qui menacent la sécurité de l'information.

Les incidents de cybersécurité constituent une faible partie des événements.

Figure 4 – Événements de cybersécurité et incidents de cybersécurité[xix]



GESTION DES INCIDENTS DE CYBERSÉCURITÉ

Processus de détection, de signalement, d'évaluation, d'intervention, de traitement des incidents de cybersécurité, et qui permet d'en tirer des leçons.

INTERVENTION EN CAS D'INCIDENT

Mesures prises pour protéger et rétablir les conditions de fonctionnement normales d'un système d'information et des renseignements qui y sont stockés lors d'un incident de cybersécurité.

ÉQUIPE D'INTERVENTION EN CAS D'INCIDENT (EII)

Équipe de l'organisation dont les membres sont suffisamment compétents et dignes de confiance et qui prend en charge les incidents pendant leur cycle de vie.

Lorsque vous détectez un incident de cybersécurité, communiquez immédiatement avec votre conseiller juridique pour obtenir des consignes sur la façon d'appliquer les dix mesures suivantes :[xx]

- Consigner la date et l'heure où l'infraction a été découverte.
- Alerter et mobiliser tous les membres de l'équipe d'intervention pour qu'ils lancent le plan de préparation.
- Sécuriser le périmètre du lieu où a eu lieu l'infraction à la sécurité des données afin de conserver les éléments de preuve.
- Empêcher toute autre perte de données. Mettre tous les systèmes informatiques touchés hors tension.
- Documenter tous les éléments connus au sujet de l'infraction.
- Interviewer toutes les personnes visées par la découverte de l'infraction et celles qui pourraient posséder de l'information à ce sujet.
- Examiner les protocoles touchant la dissémination de l'information au sujet de l'infraction pour toutes les personnes visées au tout début du processus.
- Évaluer les priorités et les risques d'après ce que vous savez au sujet de l'infraction.
- Informer les autorités compétentes, y compris votre organisme de réglementation.
- Aviser les organismes d'application de la loi, le cas échéant, pour qu'une enquête approfondie soit ouverte.

Les cinq phases de la gestion d'un incident de cybersécurité sont présentées à la Figure 5 ci-dessous.

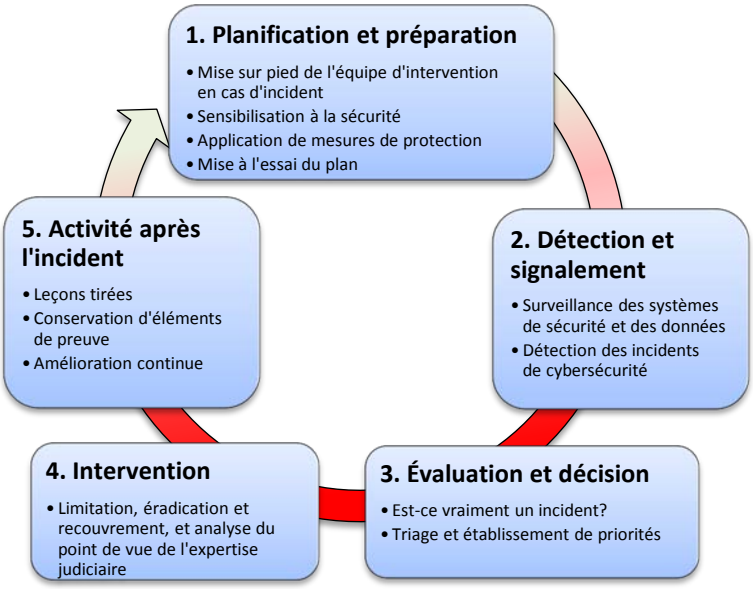


Figure 5 - 5 éléments clés de la gestion d'un incident de cybersécurité

1. La première phase comprend la **planification et** la **préparation** pour que votre organisation soit prête en cas d'incident de cybersécurité.
2. La phase de **détection et** de **signalement** comprend la surveillance permanente des sources d'information, la détection d'un événement de cybersécurité, et la collecte et la consignation de l'information associée à l'événement.

3. La phase d'**évaluation et** de **décision** comprend l'évaluation des événements de cybersécurité et la décision à savoir si un incident de cybersécurité est survenu.
4. La phase d'**intervention** comprend la limitation et l'atténuation d'un incident de cybersécurité, et la reprise des activités après l'incident.
5. L'**activité après l'incident** comprend les leçons tirées de l'incident et les changements apportés en vue d'accroître la sécurité de l'organisation et d'améliorer ses processus.

➔ **L'annexe A renferme une *liste de contrôle d'un incident de cybersécurité.***

3.12 Partage de l'information et signalement d'une infraction

3.12.1 Avis d'infraction à la sécurité

En juin 2015, la *Loi sur la protection des renseignements personnels numériques* a modifié une loi canadienne fondamentale, la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), pour indiquer que l'organisation devra aviser le commissaire à la protection de la vie privée et les personnes visées de « toute atteinte aux mesures de sécurité qui a trait à des renseignements personnels dont elle a la gestion, s'il est raisonnable de croire, dans les circonstances, que l'atteinte présente un risque réel de préjudice grave à l'endroit d'un individu. » La *Loi sur la protection des renseignements personnels numériques* prévoit des amendes pouvant atteindre 100 000 $ pour le non-respect en connaissance de cause des exigences de signalement d'une infraction aux mesures de sécurité, et l'exigence de conserver et de tenir à jour un registre des infractions concernant les mesures de sécurité portant sur les renseignements personnels dont l'organisation a la garde.

Les exigences de notification comprises dans les règlements qui ne sont pas encore promulgués ne seront pas mises en vigueur. Il est évident que le non-respect des exigences canadiennes de signalement d'une infraction évolue et que les sociétés canadiennes doivent faire preuve de vigilance à cet égard.

Les dispositions de la LPRPDE ne s'appliquent pas dans les provinces qui disposent de lois sur la protection des renseignements personnels qui, de l'avis du gouvernement fédéral, sont essentiellement semblables à la LPRPDE. À l'heure actuelle, seules les provinces de l'Alberta, de la Colombie-Britannique et du Québec appliquent de vastes lois sur la protection des renseignements personnels déclarées essentiellement semblables à la LPRPDE. Mais seule la loi de l'Alberta renferme des dispositions de signalement obligatoire des infractions aux mesures de sécurité. Les sociétés ont l'obligation d'être au courant du signalement d'une infraction dans chacun des territoires où elles exercent des activités et d'appliquer des politiques internes conformes aux lois applicables.

3.12.2 Échange de renseignements

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 de renseignements est un élément essentiel d'un programme efficace de cybersécurité. De plus en plus dans le secteur financier, la cybersécurité est perçue comme un bien collectif par les intervenants du marché. Des doutes au sujet de l'intégrité d'un intervenant peuvent rapidement en toucher d'autres. On note un empressement à participer au partage des pratiques exemplaires en cybersécurité et des renseignements sur les menaces entre les membres du secteur financier.

En outre, le libellé de la *Loi sur la protection des renseignements personnels numériques* est plus permissif que celui des lois antérieures et il permet aux organisations de partager entre elles des renseignements afin de détecter ou de supprimer les possibilités de fraude. Il est également plus permissif au chapitre du partage de renseignements dans le cadre d'une enquête sur une

infraction, ou une attente raisonnable d'infraction à un accord ou à une loi du Canada ou d'une province. Même si les lois antérieures exigeaient l'existence d'un organisme d'enquête accrédité, la nouvelle loi semble permettre aux secteurs de partager plus efficacement des renseignements sur la cybersécurité ou d'autres renseignements liés à la sécurité dans le but de protéger leurs intérêts. Le secteur canadien des valeurs mobilières est bien positionné pour suivre les secteurs des services bancaires et des assurances afin de mettre en place des ententes spéciales et structurées de partage des renseignements à l'appui des programmes de cybersécurité des sociétés.

Le partage ou l'échange de renseignements constitue un outil essentiel d'atténuation des menaces de cybersécurité. Il embrasse les niveaux stratégiques, tactiques, opérationnels et techniques, de même que toutes les phases du cycle d'intervention en cas d'incident. Il transcende les frontières des domaines public et privé. Enfin, il porte sur les renseignements de nature délicate, ce qui peut être nuisible pour une organisation, tout en étant très utile à d'autres.[xxi]

Pour les courtiers membres, il existe diverses possibilités et tribunes de partage proactif des renseignements. Sécurité publique Canada exploite le Centre canadien de réponse aux incidents cybernétiques (CCRIC) dans le but exprès de faciliter le cyberéchange de renseignements entre les secteurs canadiens et avec le gouvernement du Canada. Le Centre comprend l'un des laboratoires de lutte aux programmes malveillants les plus modernes du Canada et il peut fournir une aide précieuse aux courtiers membres qui ont été victimes de cybermenaces.

Le Financial Services Information Sharing and Analysis Center (FS-ISAC) est une ressource mondiale de partage de renseignements visant précisément les cybermenaces et les menaces physiques dirigées contre la communauté financière mondiale. Le FS-ISAC recherche constamment auprès de ses membres des données sur les menaces qui pourraient les toucher, afin d'émettre des avis proactifs sur d'éventuelles menaces.

Les exemples qui précèdent ne représentent que deux des nombreuses collectivités qui partagent des renseignements et pratiques exemplaires de cybersécurité. Ces collectivités appliquent le principe selon lequel la cybersécurité efficace est un bien collectif et qu'un incident de sécurité dans une institution constitue le rapport de pré-alerte de la collectivité. Les courtiers membres sont invités à appuyer ces collectivités à l'aide de rapports d'incident pertinents et à mettre à contribution les renseignements reçus dans le cadre du partage de l'information afin d'optimiser leurs programmes de cybersécurité.

Microsoft formule les huit recommandations qui suivent pour le partage des renseignements.[xxii]

1. **Élaborer une stratégie de partage de l'information et de collaboration**.
    a. Une stratégie de partage de l'information peut aider une organisation : cerner les priorités, déterminer des valeurs partagées et prévoir de mettre au point des processus efficaces de partage de l'information.
    b. La stratégie de partage de l'information devrait répondre aux questions suivantes :
        i. Qui doit partager l'information, et qui peut résoudre les problèmes éventuels?
        ii. Quels renseignements sont partagés, et dans quel but?

iii. Quelle est la motivation qui sous-tend le partage de l'information? L'information est-elle partagée sur une base volontaire ou s'agit-il d'une obligation réglementaire?
iv. Quelle est la structure de partage de l'information au sein de l'organisation?
v. Comment l'information est-elle partagée de façon sûre?
vi. Comment l'échange de renseignements est-il structuré pour en optimiser la valeur?

2. **Concevoir en tenant compte de la protection des renseignements personnels.**
Les projets de partage de l'information doivent respecter la vie privée et doivent être conçus dans le but d'offrir une protection maximale.

3. **Établir un processus de gouvernance significatif.**
Le respect des règles de partage de l'information par les membres est essentiel pour la crédibilité de l'initiative et le raffermissement de la confiance. Un processus de gouvernance significatif prévoit la gestion efficace des données partagées, à partir de leur création jusqu'à leur destruction, en passant par leur diffusion et leur utilisation.

4. **Insister sur le partage des renseignements sur les menaces, les vulnérabilités et l'atténuation pouvant servir à la mise en place de mesures.**
Le partage de renseignements pouvant servir à la mise en place de mesures permet à l'organisation d'améliorer la défense de ses réseaux et d'atténuer les menaces.

5. **Bâtir des relations interpersonnelles.**
Il est essentiel d'établir une relation de confiance entre les participants au processus de partage de l'information, de même que la confiance dans le programme proprement dit. Le partage de renseignements de bonne foi entre les participants peut inciter davantage de participants à prendre part au partage de l'information sur les menaces et les vulnérabilités.

6. **Limiter le partage de l'information à des circonstances précises.**
Dans certains cas, notamment lorsqu'il s'agit de la sécurité nationale et de la sûreté publique, il se peut que le signalement d'un incident soit obligatoire. Une telle démarche doit être définie de façon stricte et être mise en œuvre dans le cadre de mécanismes dignes de confiance.

7. **Garantir le partage de l'information, en effectuant des analyses sur les tendances à long terme**.
Une analyse des tendances recueillies à partir de renseignements partagés peut permettre de mieux cerner les tendances à long terme, aider les défenseurs des réseaux à mieux comprendre les nouvelles cybermenaces et à se défendre contre les menaces futures ou les prévenir.

8. **Encourager le partage des pratiques exemplaires**.
   L'échange des pratiques exemplaires avec des organisations peut permettre à ces dernières de jouer un rôle actif entre elles et avec des organisations de l'extérieur.

3.13 Cyberassurance

L'assurance liée aux infractions à la sécurité des données en vertu des polices commerciales traditionnelles est devenue de plus en plus incertaine. Au début des années 2000, les sociétés d'assurances ont commencé à offrir des polices portant spécifiquement sur la protection contre les pertes financières engendrées par des infractions à la sécurité des données.

Les types de risques et les pertes éventuelles sont :

- Le vol d'identité
- L'interruption des activités
- Les dommages causés à la réputation et à la clientèle
- Le coût des enquêtes et des correctifs
- Le coût de remplacement des biens
- Le vol de biens numériques
- Les programmes malveillants et les virus
- L'erreur humaine
- Le coût de règlement des litiges

La protection d'assurance liée à certaines pertes peut être offerte dans le cadre de certaines polices de type traditionnel :

- Administrateurs et dirigeants (A et D)
- Erreurs et omissions (E et O) / Responsabilité professionnelle
- Crime / Vol
- Biens
- Responsabilité civile générale (RCG)

Dans bien des cas, l'assurance traditionnelle n'embrasse pas toute la gamme des risques et les pertes éventuelles que posent les cyberrisques. À l'étape de l'examen des assureurs éventuels, il importe de savoir que cette sous-spécialité demeure à l'étape de l'élaboration; il n'existe donc pas de clauses standard au sein du secteur.

Une pratique exemplaire consiste à examiner minutieusement les dispositions des polices d'assurance générale de la société et des administrateurs et dirigeants en ce qui concerne les demandes de règlement pour infractions à la sécurité des données et à la protection des renseignements personnels, et à veiller à ce qu'aucune demande de ce type ne soit exclue. Dans le cadre d'une vaste stratégie de cybersécurité, il convient de déterminer le type et la portée de la protection qui correspond le mieux aux intérêts de l'entreprise, et de chercher une police d'assurance adaptée qui englobe tous les risques auxquels un cyberincident pourrait exposer l'entreprise.

Une protection rétroactive constitue une importante possibilité. Il faut compter des mois, voire des années, avant de découvrir des cyberinfractions; par conséquent, les membres doivent savoir qu'ils ont peut-être déjà été victimes d'une infraction non détectée lorsqu'ils soumettent une demande de police d'assurance. Dans certains cas, les sociétés d'assurance accepteront d'offrir une protection rétroactive pouvant atteindre deux ans avant de souscrire une police. Cet avenant dépend dans une large mesure du profil de risque exclusif de l'assuré éventuel et de la nature du programme de cybersécurité.

Une protection type offerte dans le cadre de polices de cybersécurité peut comprendre les éléments suivants :

Exemples de protection de cyberassurance

Protection de première partie	**Protection en responsabilité civile**
Embauche d'un professionnel : • Avocat-conseil • Cabinet de relations publiques • Cabinet de gestion de crise • Cabinets spécialisés dans l'expertise judiciaire Coûts liés aux avis : • Coûts directs, y compris l'impression/l'envoi postal • Services de surveillance du crédit pour les personnes touchées Coût de protection administrative : • Formation des employés • Création de portails d'information • Création de modèles de sécurité et d'intervention en cas d'incident • Dédommagement des assurés pour la perte de revenu imputable à une infraction • Récupération des données perdues	• Coût de défense réglementaire, y compris les amendes et les dommages-intérêts punitifs • Coût de défense contre les litiges • Dommages-intérêts à l'issue de litiges

3.14 Gestion des risques de fournisseur

Le nombre d'incidents de sécurité survenus dans des sociétés et qui sont imputables aux systèmes des clients, des partenaires et des fournisseurs est passé de 20 % en 2010 à 28 % en 2012.[xxiii] L'exemple le plus connu de risque de fournisseur est l'infraction massive touchant les données de Target Corp, en 2013; à cette occasion, des pirates ont obtenu l'accès aux données de cartes de crédit grâce à un sous-traitant du domaine du chauffage et de la climatisation. Jusqu'à 40 millions de numéros de carte de crédit et de débit ont été exposés.

Les éléments essentiels d'un programme de gestion des risques de fournisseur comprennent le classement des fournisseurs en fonction des risques, l'établissement de politiques précises que les fournisseurs doivent respecter, l'intégration de conditions explicites dans les contrats, et la mise au point d'un programme visant à vérifier le rendement des fournisseurs.

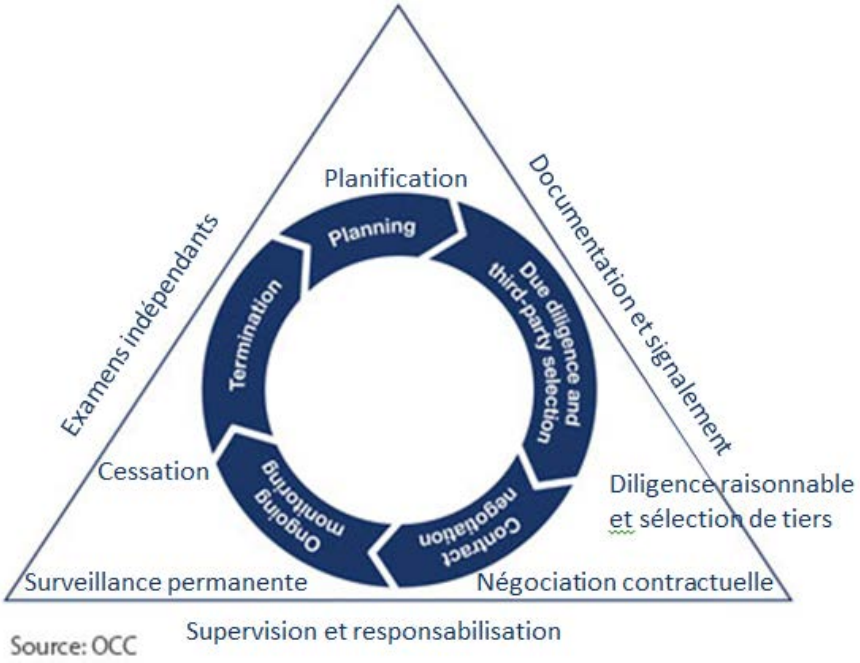


Figure 6 – Cycle de la gestion des risques pour le risque de tiers
Office of the Comptroller of the Currency (OCC)

De nos jours, il est presque impossible de trouver une entreprise qui ne s'en remet pas à des fournisseurs. Compte tenu du risque que pose la relation avec un tiers fournisseur, les entreprises intègrent les pratiques de sécurité de ces fournisseurs dans leur propre profil de risque. L'Office of the Comptroller of the Currency (OCC), des États-Unis, a élaboré un excellent cadre permettant de créer un programme efficace de gestion du risque de fournisseur (voir la Figure 6 ci-dessus). Ce modèle de cycle de vie souligne les principales étapes de planification préliminaire, de diligence et de négociation pour 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 cessation de la relation pour que l'accès aux réseaux soit interrompu et que les données confidentielles soient retournées.

Une pratique exemplaire consiste à envisager la gestion du risque de fournisseur par niveau, le premier étant réservé aux relations posant le plus grand risque. La stratification des fournisseurs[xxiv] peut être envisagée sous l'angle des considérations suivantes :

Risques liés au service :

- Volume d'opérations financières traitées
- Concentration associée aux services
- Risque lié à la sensibilité des données auxquelles le fournisseur pourrait avoir accès
- Risque de conformité et risque réglementaire se rapportant au service
- Impact financier et conséquences pour la clientèle

Risques liés au fournisseur :

- Emplacement du fournisseur (sous réserve des lois et règlements multinationaux, etc.)
- Infractions antérieures à la sécurité ou à la sécurité des données
- Portée de l'impartition exécutée par le fournisseur
- Historique du rendement

Lacunes courantes des tiers fournisseurs :

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

Les approches courantes d'évaluation des tiers fournisseurs comprennent :

- Questionnaires intégrés aux demandes de propositions
    - Un modèle de questionnaire d'évaluation des fournisseurs figure à l'Annexe B.
- Demandes de documentation aux fournisseurs éventuels
    - Le modèle de questionnaire d'évaluation des fournisseurs présenté à l'Annexe B renferme des exemples de ces types de documentation.
- Évaluations administratives pour déterminer la valeur des renseignements demandés
- Visites sur place par des experts à l'interne ou de l'extérieur
- Tests de pénétration portant sur les fournisseurs éventuels

Pour être efficace, la gestion des risques de fournisseur devrait être intégrée au programme de gestion des risques de l'organisation et comporter des processus établis et répétitifs uniformes dans tous les services de l'organisation.

Étude de cas – « Piratage à des fins de court-circuitage » - 2010 à 2014

Sur une période de cinq ans s'échelonnant de 2010 à 2014, des pirates étrangers de mèche avec des initiés des États-Unis ont volé des renseignements d'entreprise non publics et ont effectué des tentatives payantes en infiltrant les serveurs de PRNewswire Association LLC, Marketwired LP et Business Wire.

Les suspects ont eu recours à des techniques d'hameçonnage et ont planté un code de programmation malveillant dans des applications ou des sites Internet pour avoir accès aux bases de données renfermant les communiqués des entreprises susmentionnées. Ils ont ensuite tiré profit de la période comprise entre le moment où les sociétés désignées ont téléchargé les communiqués dans des fils de presse et la diffusion du contenu des communiqués dans le public.

Ce stratagème représente la plus importante collaboration connue entre des pirates et des initiés; ils ont engrangé des profits illégaux de 30 millions de dollars. Cette démarche a souligné le danger invisible des finances modernes et de l'Internet; un lien compromis dans la vaste chaîne peut lentement mettre le système en danger pendant des années.

3.14.1 Infonuagique

Dans sa forme la plus simple, l'infonuagique correspond au stockage des données et à leur accès sur Internet plutôt que sur le lecteur d'un ordinateur.[xxv] Même si ce concept présente de nombreux avantages, il comporte des risques semblables à ceux associés à l'impartition à des fournisseurs tiers; toutefois, contrairement aux fournisseurs tiers, la principale activité d'un fournisseur de services d'infonuagique est le stockage d'applications essentielles et de données de nature délicate. Par conséquent, la protection de la sécurité et des données constitue la principale préoccupation de la plupart des entreprises qui envisagent de recourir à cette option. Les entreprises doivent tenir compte des risques et de 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.

Outre les directives concernant l'atténuation des risques, énoncées à la section portant sur la gestion des fournisseurs, les entreprises qui envisagent de souscrire à des services d'infonuagique doivent trouver un fournisseur aux caractéristiques suivantes :[xxvi]

- D'importants antécédents dans le domaine des services d'infonuagique qui peuvent fournir des références professionnelles solides
- Le fournisseur énonce clairement ses contrôles d'atténuation au chapitre de la gestion des risques – contrôles se rapportant à la sécurité, à la disponibilité, à l'intégrité du traitement, à la confidentialité et à la protection des renseignements personnels
- Le fournisseur peut auditer et vérifier 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 reprise des activités et ses plans de reprise après sinistre respectent les exigences de votre entreprise.

3.15 Politique de cybersécurité

Un programme de cybersécurité est défini par la politique qui le sous-tend. La politique de sécurité de l'organisation constitue la pièce maîtresse des objectifs de la société, qui ont été convenus par la direction et qui établissent les exigences qui doivent être respectées. Plutôt que des orientations ou des lignes directrices, **la politique établit une conduite obligatoire**.

La création d'une politique de sécurité exige que la direction énonce ce qu'elle estime nécessaire et les risques qu'elle est disposée à assumer, plutôt que de simplement « télécharger » un modèle de politique de sécurité. Une pratique exemplaire consiste à mobiliser la direction de l'organisation dans le cadre d'un processus de sensibilisation au sujet des risques de sécurité afin d'établir un consensus éclairé entre les membres de la haute direction et avec eux, qui constituent l'autorité sur laquelle reposent l'élaboration et l'exécution de la stratégie de cybersécurité.

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 l'appui des pratiques de continuité 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 disciplines de la sécurité.

Les principaux éléments d'une politique de sécurité comprennent :

- La portée – 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'extérieur), sans exception
- La classification de l'information – doit fournir des définitions axées sur le contenu plutôt que des définitions plus générales de type « confidentiel » ou « restreint »
- Les objectifs de la direction au chapitre de la manutention protégée de l'information dans chacune des catégories de la classification
- La place de la politique dans le contexte des autres directives et documents de la direction
- Les renvois aux documents d'appui, notamment les normes et lignes directrices du secteur
- Des instructions précises au sujet de mandats de sécurité à la grandeur de l'organisation (p. ex., aucun partage des mots de passe)

- La désignation spécifique 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)[xxvii]

La mise en œuvre d'une politique ne constitue pas un événement unique; il s'agit plutôt d'un processus itératif réexaminé au fil de l'évolution des modèles de l'entreprise, des relations et des changements technologiques. **En l'absence d'une politique, la gouvernance du programme de cybersécurité ne peut être efficace, car il n'existe pas d'orientations ou de lignes directrices précises qui permettent de prendre des décisions relatives aux programmes.**

Annexe A – Liste de contrôle d'un incident de cybersécurité

Vous trouverez ci-dessous les processus et procédures qui doivent être en place avant, pendant et après un incident de cybersécurité[xxviii]:

LISTE DE CONTRÔLE D'UN INCIDENT DE CYBERSÉCURITÉ

AVANT UN INCIDENT

- ☐ Dresser une liste priorisée des actifs informationnels d'une importance critique pour le bon fonctionnement de votre organisation.
- ☐ Identifier les intervenants responsables de chaque actif d'une importance critique.
- ☐ Mettre sur pied une équipe d'intervention en cas d'incident qui sera chargée de tous les incidents (comprenant des représentants des services juridiques, des communications et des ressources humaines).
- ☐ Veiller à ce que des technologies pertinentes de surveillance et de suivi soient en place pour protéger les actifs informationnels de votre organisation (notamment des pare-feu, des systèmes de prévention des intrusions (SPI) et des antivirus).
- ☐ Fournir une formation média aux personnes compétentes.
- ☐ Mettre en place un processus à la grandeur de l'organisation pour permettre aux employés, aux sous-traitants et aux tiers de signaler les activités suspectes ou les soupçons de piratage.
- ☐ Donner de la formation dans toute l'organisation au sujet de la sensibilisation aux infractions, de la responsabilité des employés et des processus de signalement.

PENDANT UN INCIDENT

- ☐ Consigner les problèmes et préparer un rapport d'incident.
- ☐ Convoquer l'équipe d'intervention en cas d'incident (EII).
- ☐ Organiser une téléconférence avec les intervenants compétents pour discuter

des mesures à prendre pour rétablir les activités.

- Organiser une téléconférence avec les intervenants compétents pour faire le point sur la situation avec la haute direction.
- Trier les enjeux actuels et les communiquer à la haute direction.
- Déterminer la cause initiale de l'incident et convoquer les spécialistes pour corriger les problèmes afin de rétablir les activités.
- Conserver les éléments de preuve et suivre une chaîne de preuves rigoureuse à l'appui de toute mesure juridique nécessaire ou prévue.
- Communiquer avec les tiers visés, les organismes de réglementation et les médias (si nécessaire).

APRÈS UN INCIDENT

- Mettre à jour le rapport d'incident et déterminer exactement ce qui est arrivé et à quel moment.
- Vérifier dans quelle mesure le personnel et la direction ont bien agi au cours de l'incident.
- Déterminer si les procédures documentées ont été suivies.
- Discuter des changements qu'il faudra apporter aux processus ou à la technologie pour atténuer les incidents futurs.
- Déterminer les renseignements qui auraient dû être fournis plus tôt.
- Déterminer si les étapes appliquées ou les mesures prises auraient pu nuire à la reprise.
- Préciser les outils ou autres ressources nécessaires pour détecter, trier, analyser et atténuer les incidents futurs.
- Discuter des exigences de signalement nécessaires (notamment au chapitre de la réglementation et de la clientèle).
- Dans la mesure du possible, quantifier les pertes financières causées par l'infraction.

Annexe B – Modèle de questionnaire d'évaluation des fournisseurs

Adaptation du Third-Party Assessment Questionnaire, University of British Columbia.[xxix]

L'original peut être consulté à l'adresse suivante : https://it.ubc.ca/sites/it.ubc.ca/files/3rd%20Party%20Outsourcing%20Information%20Security%20Assessment%20Questionnaire%20V1.4.xlsx

Sources additionnelles :

- Gestion des fournisseurs de l'ISACA à l'aide de COBIT 5[xxx]
- Questionnaire sur l'initiative d'évaluation consensuelle de la Cloud Security Alliance V3.0.1[xxxi]

Modèle de questionnaire d'évaluation des fournisseurs

Raison sociale	
Courriel Numéro de téléphone Site Internet de la société	
Date de l'évaluation	

Documents additionnels fournis	☐ Diagramme du réseau ☐ Architecture de sécurité ☐ Résultats de l'évaluation de la sécurité ☐ Politiques de sécurité ☐ Rapports ISO, SAE16 ☐ Politique de gestion des risques ☐ Politique de gestion des fournisseurs ☐ Plan de gestion du changement ☐ Procédures de sauvegarde et de rétablissement ☐ Politique de conservation des documents ☐ Plan de gestion des incidents ☐ Plan de continuité des activités ☐ Plan de reprise après sinistre ☐ Procédures d'évaluation des risques ☐ Autres documents pertinents

Contrôles chez le fournisseur	Réponse du fournisseur Oui/Non/Mise en œuvre partielle
1. Permet l'audit de sécurité sur place avec préavis de 24 heures	
2. Stocke toutes les données au Canada	
3. Tient un registre d'audit pour la localisation de toutes les données confidentielles.	
4. N'accédera pas à des données confidentielles de l'étranger	
5. Peut fournir les résultats récents de l'évaluation externe de la sécurité de l'information	
6. Tient à jour des procédures d'intervention en cas d'incident	
7. Applique une politique de protection des renseignements sur le client contre l'accès non autorisé	
8. Applique une politique qui interdit le partage de comptes et de mots de passe personnels	
9. Applique une politique qui met en œuvre les principes du besoin de savoir et de la division des tâches	
10. Applique un processus d'authentification plurifactorielle pour l'accès aux ressources du client	
11. Vérifie les antécédents de tous les employés	
12. Fournit un soutien à la clientèle et a prévu une procédure de signalement	
13. Dispose de processus documentés de contrôle du changement	
14. Oblige les employés à assister à des séances périodiques de sensibilisation et de formation en sécurité	
Architecture de sécurité	**Réponse du fournisseur** **Oui/Non/Mise en œuvre partielle**
1. Fournira un diagramme de topologie du réseau	
2. A mis en œuvre une protection réseau au moyen de pare-feu	
3. A mis en œuvre une protection de pare-feu pour les applications Web	
4. Protège les systèmes hôte au moyen de pare-feu	
5. Prévoit la redondance du réseau	
6. A mis en place une technologie de systèmes de prévention des intrusions	
7. A mis en œuvre une architecture DMZ par paliers pour les systèmes fondés sur Internet	
8. Utilise une protection virus intégrée pour tous les systèmes	
9. Applique un programme de gestion des correctifs	
10. Offre des serveurs clients désignés afin de séparer les données des autres données sur les clients, sinon, comment cette mesure est-elle appliquée dans une configuration virtuelle ou segmentée protégée?	
11. Met en œuvre des contrôles pour limiter l'accès aux données d'autres clients	

12. L'accès à distance s'effectue au moyen de connexions protégées qui utilisent l'authentification plurifactorielle	
13. L'élaboration, la mise à l'essai et le mode de production sont séparés physiquement ou virtuellement	
14. Utilise des points d'accès gérés et protégés sur son réseau sans fil	

Configuration des systèmes d'information	Réponse du fournisseur Oui/Non/Mise en œuvre partielle
1. Met en œuvre le chiffrement des renseignements confidentiels à un niveau minimal de AES 128 octets et TLS 1.0	
2. Dispose d'écrans de veille protégés par mot de passe qui s'activent automatiquement pour empêcher l'accès non autorisé aux systèmes	
3. Utilise des logiciels de surveillance de l'intégrité des fichiers sur les serveurs (notamment Tripwire, etc.)	
4. Utilise des mots de passe d'au moins dix caractères dont les exigences de complexité doivent être modifiées aux 90 jours	
5. Veille à ce que le mot de passe ne soit jamais archivé sous forme de texte en clair	
6. Met en œuvre la redondance ou la disponibilité élevée pour les fonctions essentielles	
7. N'utilise pas de données de production dans les modes de développement et d'essai	
8. Active la fonction de blocage de compte pour les échecs répétitifs de branchement sur tous les ordinateurs d'appui du système	
9. Interdit la tunnelisation partagée lors du branchement aux réseaux des clients	
Contrôles d'accès	**Réponse du fournisseur** **Oui/Non/Mise en œuvre partielle**
1. Supprime ou modifie immédiatement l'accès lorsqu'un employé quitte son poste, est muté ou change de fonctions	
2. Veille à ce qu'au moins deux personnes autorisées et dignes de confiance aient accès aux données ou systèmes essentiels pour éviter une panne à un point de service	
3. Veille à ce que les utilisateurs ne disposent que de l'autorisation de lecture ou de modification des programmes ou des données nécessaires pour exécuter leurs tâches	
Surveillance de la sécurité	**Réponse du fournisseur** **Oui/Non/Mise en œuvre partielle**
1. Examine périodiquement les permissions d'accès pour tous les fichiers, bases de données et applications du serveur	
2. Examine et analyse périodiquement l'accès aux systèmes après les heures normales	
3. Examine périodiquement les registres des systèmes pour repérer les échecs de branchement ou les tentatives d'accès qui ont échoué	
4. Examine et supprime périodiquement les comptes inactifs dans les systèmes	
5. Examine périodiquement les registres de réseau et de pare-feu	
6. Examine au moins périodiquement les registres d'accès sans fil	
7. Recherche périodiquement les points d'accès non autorisés	

Sécurité physique	Réponse du fournisseur Oui/Non/Mise en œuvre partielle
1. Contrôle l'accès aux zones protégées	
2. Contrôle l'accès aux salles de serveur et applique les principes du privilège minimum et du besoin de savoir	
3. A mis en place des mesures de sauvegarde (p. ex., serrures à code, accès restreint, registre d'accès aux salles, contrôle d'accès par carte glissée)	
4. Déchiquette ou brûle les documents d'information confidentiels	
5. Accompagne les visiteurs dans les salles d'ordinateur et les zones de serveur	
6. Met en œuvre des contrôles environnementaux afin d'atténuer les menaces environnementales au matériel	
Planification d'urgence	**Réponse du fournisseur** **Oui/Non/Mise en œuvre partielle**
1. Applique un plan d'urgence écrit aux activités informatiques essentielles pour la mission	
2. Met à jour le plan d'urgence au moins une fois l'an	
3. Applique des procédures et processus de sauvegarde écrits	
4. Vérifie l'intégrité des supports de sauvegarde une fois par trimestre	
5. Archive le support de sauvegarde de façon protégée et en contrôle l'accès	
6. Tient à jour un plan de reprise après sinistre documenté et vérifié	
7. Fournit des avis en cas d'infraction à la sécurité	
8. Le fournisseur a-t-il été victime d'une infraction à la cybersécurité au cours des trois à cinq dernières années? 9. Dans l'affirmative, veuillez indiquer les renseignements perdus dans la section réservée aux commentaires	
Associés du fournisseur	**Réponse du fournisseur** **Oui/Non/Mise en œuvre partielle**
1. Des ententes de confidentialité ont été signées avant que des renseignements exclusifs et/ou confidentiels aient été divulgués aux associés du fournisseur.	
2. Des contrats ou ententes avec les associés du fournisseur sont en vigueur et protègent convenablement contre les risques reliés aux besoins des consommateurs	
3. Les associés du fournisseur sont au courant des politiques de sécurité des clients et de ce que l'on attend d'eux	
4. Les ententes avec les associés du fournisseur documentent le transfert convenu des données des clients lorsque la relation d'affaires est rompue	

Annexe C – Glossaire

La présente section s'inspire du guide du gouvernement du Canada intitulé *Pensez cybersécurité pour les petites et moyennes entreprises* à titre de source faisant autorité pour permettre au lecteur de mieux comprendre les termes et expressions clés utilisés dans le présent document.

Actif : Élément ou article appartenant à la société ou qu'elle a en sa possession et qui présente une certaine valeur (notamment des renseignements, sous toutes formes et sur tous systèmes).

Attaque : Tentative d'obtenir l'accès non autorisé à des renseignements personnels ou propres à la société, à des systèmes ou réseaux informatiques dans un dessein (habituellement) criminel. Une attaque réussie peut se traduire par une atteinte à la sécurité ou être généralement considérée comme un « incident ».

Authentification : Pratique de sécurité (prenant habituellement la forme d'un contrôle logiciel) visant à confirmer l'identité d'une personne avant de lui donner accès aux services, ordinateurs ou renseignements de la société.

Cyber : Relatif aux ordinateurs, aux logiciels, aux systèmes de communication et aux services utilisés pour avoir accès à Internet et interagir sur la toile.

Chiffrement : Conversion d'une information en code ne pouvant être lu que par les personnes autorisées et qui ont reçu la « clé » nécessaire (et habituellement unique) et les logiciels spéciaux de manière à pouvoir renverser le processus (p. ex., le déchiffrement) et utiliser l'information.

Correctif : Mise à jour ou réparation d'une forme de logiciel appliquée sans remplacement du programme original. De nombreux correctifs sont fournis par des développeurs de logiciels pour corriger des vulnérabilités de sécurité connues.

Hameçonnage : Type précis de pourriel qui cible une ou plusieurs personnes et qui se présente sous une forme légitime, dans le but de frauder le destinataire ou les destinataires.

Infraction à la sécurité : Problème de sécurité imputable à la négligence ou à une attaque délibérée. Il peut s'agir d'une action contraire à une politique ou à une loi, et elle est souvent exploitée pour favoriser une autre action nuisible ou criminelle.

Logiciel malveillant : Logiciel créé et distribué à des fins malveillantes. Le plus souvent, ce type de logiciel prend la forme d'un « virus ».

Menace : Événement ou acte potentiel (délibéré ou accidentel) qui pose un danger pour la sécurité de l'organisation.

Mesure de protection : Processus de sécurité, mécanisme physique ou outil technique servant à éliminer des menaces précises. Parfois désigné *contrôle*.

Mot de passe : Mot secret ou combinaison de caractères secrets utilisés pour authentifier leur utilisateur.

Pare-feu : Type de barrière de sécurité placée entre divers réseaux. Il peut s'agir de dispositifs dédiés ou d'un ensemble de composantes et techniques. Seules les opérations autorisées, définies par la politique de sécurité locale, sont autorisées.

Pourriel : Courriel envoyé sans la permission du destinataire ou que celui-ci n'a pas demandé.

Risque : Exposition à un résultat négatif si une menace se concrétise.

RPV : Réseau privé virtuel.

Sauvegarde : Processus qui consiste à copier des fichiers dans un dispositif de stockage secondaire, pour que ces fichiers soient accessibles en cas de besoin (p. ex., après une panne d'ordinateur).

Serveur : Ordinateur membre d'un réseau qui fait fonction de ressource partagée pour d'autres processeurs rattachés au réseau (pour stocker et « servir » des données ou des applications).

Vol d'identité : Copie des renseignements identitaires d'une personne (notamment son nom et son numéro d'assurance sociale) pour se faire passer pour elle afin de commettre un acte de fraude ou une autre activité criminelle.

Vulnérabilité : Faiblesse du logiciel, du matériel, de la sécurité physique ou des pratiques humaines qui peut être exploitée pour lancer une attaque à la sécurité.

Wi-Fi : Réseau local (LAN) qui utilise les fréquences radio pour transmettre et recevoir des données sur une distance de quelques centaines de pieds.

Annexe D – Bibliographie

NIST Cybersecurity Framework, Version 1.0, 2014
CGI, « Cybersecurity in Modern Critical Infrastructure Environments », 2014
ENISA, « Technical Guideline on Security Measures », Version 2.0, 2014
Sécurité publique Canada. *Sécurité informatique et systèmes de contrôle industriel (SCI) Pratiques exemplaires recommandées*, 2012
xxxii xxxiii xxxiv xxxv

---

[i] Publication spéciale 800-53 du NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*
[ii] Australian Signals Directorate. *Strategies to Mitigate Targeted Cyber Intrusions*, février 2014
[iii] *Guide Pensez cybersécurité pour les petites et moyennes entreprises*
[iv] National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity,* 2014
[v] Cyber-Ark. *Security & Passwords Survey,* 2012
[vi] CERT Insider Threat Center, http://www.cert.org/insider-threat/
[vii] Bunn, C. *A Focus on Insider Threats in Banking & Financial Institutions*, 2013
[viii] Shaw, E.D. et H.V. Stock. Harley V. Stock, Ph.D. *Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property: Misreading the Writing on the Wall*, 2011
[ix] Price Waterhouse Coopers. *2015 Global State of Information Security® Survey*, 2015
[x] CyberEdge Group. *2015 Cyberthreat Defense Report: North America & Europe*, 2015
[xi] The Council On CyberSecurity. *The Critical Security Controls For Effective Cyber Defense*, 2015, pp. 27-32
[xii] Centre de la sécurité des télécommunications Canada. *Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada*, 2007, p. 5
[xiii]Sécurité publique Canada. *Sécurité informatique et systèmes de contrôle industriel (SCI) Pratiques exemplaires recommandées*, 2012
[xiv] Gouvernement du Canada. *Guide Pensez cybersécurité pour les petites et moyennes entreprises*, http://www.pensezcybersecurite.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-fr.aspx
[xv] Trend Micro. *Mobile Consumerization Trends & Perceptions: IT Executive and CEO Survey*, 2012
[xvi] Fraud Advisory Panel. *Bring your own device (BYOD) policies*, 2014
[xvii] ISACA. *Incident Management and Response*, 2012
[xviii] ISO/IEC. ISO 27035-2 (2[e] ébauche de travail), *Technologies de l'information -- Techniques de sécurité -- Gestion des incidents de sécurité de l'information – Partie 1 : Principes de gestion des incidents*
[xix] Government of South Australia. *ISMF Guideline 12aCybersecurity Incident Reporting Scheme*, 2014
[xx] Experian Data Breach Resolution. *Data Breach Response Guide*, 2013
[xxi] Luiijf, E. et A. Kernkamp. *Sharing Cyber Security Information: Good Practice Stemming from the Dutch Public-Private-Participation Approach*, mars 2015
[xxii] Goodwin, C. et J.P. Nicholas (Microsoft). *A Framework for Cybersecurity Information Sharing and Risk Reduction*, 2015
[xxiii] PwC. *Global State of Information Security Survey*, 2013.
[xxiv] Ibid.
[xxv] Eric Griffith. *What Is Cloud Computing?*, http://www.pcmag.com/article2/0,2817,2372163,00.asp, avril 2015
[xxvi] ISACA. *Security Considerations for Cloud Computing*, 2012
[xxvii] CSO Online. *How to write an information security policy*, consultable à http://www.csoonline.com/article/2124114/strategic-planning-erm/how-to-write-an-information-security-policy.html
[xxviii] Hewlett-Packard. *Executive breach response playbook: How to successfully navigate the enterprise through a serious data breach*, 2015

[xxix] University of British Columbia. *Third-Party Assessment Questionnaire* https://it.ubc.ca/sites/it.ubc.ca/files/3rd%20Party%20Outsourcing%20Information%20Security%20Assessment%20Questionnaire%20V1.4.xlsx

[xxx] ISACA. *Vendor Management using COBIT 5*, http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/VendorManagementDownload.aspx

[xxxi] Cloud Security Alliance. *Consensus Assessments Initiative Questionnaire V3.0.1.* https://downloads.cloudsecurityalliance.org/initiatives/cai/caiq-v3.0.1.zip

[xxxii] *http://www.antifraudcentre-centreantifraude.ca/fraud-escroquerie/types/phishing-hameconnage/index-fra.htm*

[xxxiii] *http://www.cbc.ca/news/technology/ashley-madison-data-dump-what-s-at-risk-and-for-whom-1.3199031*

[xxxiv] http://www.law360.com/articles/662840/sec-finra-officials-talks-cyberbreach-enforcement

[xxxv] *http://www.cbc.ca/news/canada/nova-scotia/cryptowall-virus-hits-some-mahone-bay-and-bridgewater-town-computers-1.3171424*

http://www.cbc.ca/news/world/100m-cybercrime-ring-busted-by-u-s-led-team-of-investigators-1.2662871