CPA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

20 Questions que les administrateurs devraient poser sur la cybersécurité

Richard Wilson

CPA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

20 Questions que les administrateurs devraient poser sur la cybersécurité

Richard Wilson

AVERTISSEMENT

La présente publication, préparée par Comptables professionnels agréés du Canada (CPA Canada), fournit des indications ne faisant pas autorité.

CPA Canada et les auteurs déclinent toute responsabilité ou obligation pouvant découler, directement ou indirectement, de l'utilisation ou de l'application de cette publication.

Préface

Le Conseil consultatif sur la surveillance et la gouvernance d'entreprises de Comptables professionnels agréés du Canada (CPA Canada) a commandé la présente publication, intitulée 20 Questions que les administrateurs devraient poser sur la cybersécurité, pour aider les administrateurs à comprendre le rôle du conseil dans la surveillance de ce risque important en constante évolution.

Le Conseil consultatif sur la surveillance et la gouvernance d'entreprises aimerait exprimer sa gratitude à l'auteur, Richard Wilson, à David Craig, Alexandre Pacheco et Vivek Jassal pour leur apport éclairé en matière de sécurité et de confidentialité, et aux permanents de CPA Canada qui ont contribué au projet et à son orientation.

Thomas Peddie, FCPA, FCA
Conseil consultatif sur la surveillance et la gouvernance d'entreprises

Auteur

Richard Wilson, CISSP

Direction du projet, CPA Canada

Stefan Mihailovich, GPLLM, CPA, CA

Gigi Dawe, LL.M.

Gord Beal, CPA, CA, M.Ed.

Conseil consultatif sur la surveillance et la gouvernance d'entreprises

Thomas Peddie, FCPA, FCA
Président

Hugh Bolton, FCPA, FCA

John E. Caldwell, CPA, CA

Andrew Foley, J.D.

Carol Hansell, LL.B., MBA, F.ICD

Bill McFarland, FCPA, FCA

Kathleen O'Neil, FCPA, FCA, ICD.D

Hari Panday, FCPA, FCGA, ICD.D

Bob Strachan, FCPA, FCMA, C.Dir

John E. Walker, CPA, CA, LL.B.

Table des matières

PARTIE A

Stratégie, gouvernance et risque en matière de cybersécurité

1. Que devraient rechercher les administrateurs dans une stratégie globale de cybersécurité?

En vue d'entamer un dialogue avec la direction sur la gouvernance de la cybersécurité, les administrateurs sont encouragés à appliquer le même cadre fondé sur le bon sens qu'ils appliquent aux autres stratégies organisationnelles. Les administrateurs peuvent sonder la direction sur les éléments qui suivent.

Stratégie de cybersécurité de la direction

a. Elle prend en considération les principaux risques liés à la cybersécurité qui pourraient directement empêcher l'organisation d'atteindre ses objectifs stratégiques. Par exemple, la stratégie de cybersécurité d'une institution financière examinerait avec soin les risques touchant son plan stratégique.

Objectif de l'entreprise de services financiers	Risque lié à la cybersécurité	Stratégie de cybersécurité
Accroître sa clientèle de détail	Vol des données bancaires des clients	Solides contrôles relatifs aux données des clients
Disposer d'informations financières exactes	Atteinte à l'intégrité des transactions	Systèmes redondants de traitement des transactions
Maintenir l'image de marque et la réputation positives de la banque	Diffusion de communications internes confidentielles de la direction	Solides contrôles relatifs à l'accès aux communications de la direction et du conseil d'administration

b. Elle classe le financement de la sécurité liée aux immobilisations et au fonctionnement des ressources, des processus et des technologies comme présentant les risques les plus élevés touchant l'organisation en matière de sécurité.

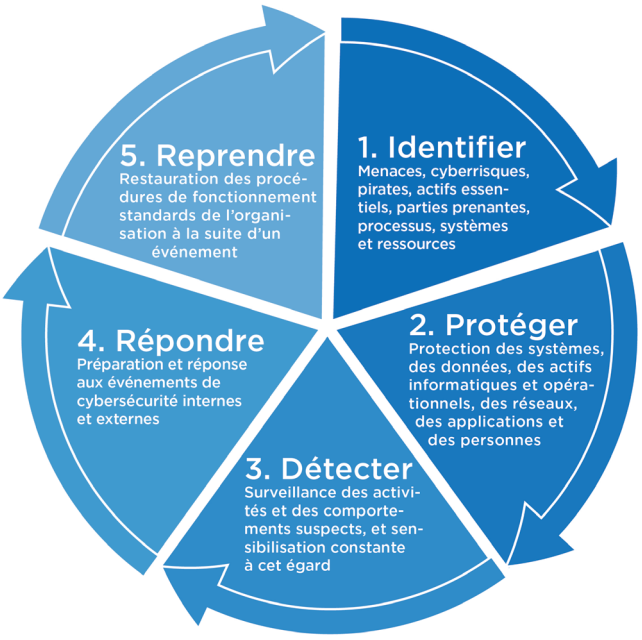
c. Elle harmonise les efforts d'un programme de cybersécurité entre :
   - les différentes divisions de l'organisation ainsi que les équipes dispersées sur le plan géographique;
   - les équipes de sécurité internes, en cotraitance et en impartition;
   - les équipes des technologies de l'information (TI) et des technologies opérationnelles (TO);
   - les programmes de cybersécurité et les programmes de protection des renseignements personnels.

Les couches du cadre de cybersécurité du National Institute of Standards and Technology

Une stratégie de cybersécurité solide combine de multiples couches de sécurité selon l'hypothèse raisonnable que, si une couche s'avère défaillante, d'autres processus, systèmes et outils sont présents pour contrecarrer une tentative d'intrusion. En s'inspirant de l'un des cadres de cybersécurité les plus reconnus, à savoir celui du National Institute of Standards and Technology (NIST), les administrateurs devraient rechercher cinq couches de protection dans une stratégie de cybersécurité efficace (voir la figure ci-après).

Le cadre de cybersécurité du NIST est intuitif comme une séquence d'étapes.

LES CINQ COUCHES DU CADRE DE CYBERSÉCURITÉ DU NIST



Cadre de cybersécurité du NIST (v1.1)

Fonction (couche) du cadre du NIST	Définition de la fonction du cadre du NIST	Catégories du cadre du NIST (par fonction)
Identifier	Afin qu'un programme de cybersécurité fonctionne efficacement, la direction doit tout d'abord identifier plusieurs composantes importantes pour consacrer temps et ressources de manière efficiente et efficace, à savoir : • les menaces et les risques internes et externes liés à la cybersécurité; • les cyberpirates internes et externes (c.-à-d. les acteurs à l'origine des menaces); • les actifs les plus importants à protéger d'une cyberattaque (p. ex. les données des clients et des employés, les systèmes informatiques essentiels, les systèmes opérationnels essentiels); • les parties prenantes responsables de l'établissement d'un programme de cybersécurité efficace; • les processus, les systèmes et les ressources qui doivent être en place pour l'établissement et l'exécution du programme de cybersécurité.	• Gestion des actifs • Contexte d'affaires • Gouvernance • Évaluation des risques • Stratégie de gestion des risques • Gestion des risques liés à la chaîne logistique
Protéger	À la suite de l'étape Identifier, la direction devrait prendre des mesures pour protéger adéquatement l'organisation. Les discussions portant sur la cybersécurité peuvent prendre une tournure très technique. Les administrateurs qui ne sont pas en mesure de discuter avec la direction sur le plan technique peuvent poser des questions au sujet des éléments suivants : • La direction a-t-elle mis en place une sécurité en vue de contrôler l'accès aux actifs physiques et numériques (c.-à-d. logiques) et aux installations qui y sont associées? L'accès est-il limité aux utilisateurs, aux processus et aux appareils autorisés, et le niveau d'accès correspond-il au niveau de risque associé à chaque actif?	• Gestion de l'identité, authentification et contrôle d'accès • Sensibilisation et formation • Sécurité des données • Processus et procédures de protection de l'information • Maintenance • Technologie de protection

Fonction (couche) du cadre du NIST	Définition de la fonction du cadre du NIST	Catégories du cadre du NIST (par fonction)
	• Des séances de formation et de sensibilisation en matière de cybersécurité sont-elles offertes au personnel et aux partenaires de l'organisation (voir Question 4)? • La sécurité des informations et des enregistrements (données) est-elle proportionnelle au niveau de risque de perte ou de compromission de ces dossiers de données? • La direction dispose-t-elle, en matière de sécurité, de politiques, de processus et de procédures appropriés qui sont suivis de manière systématique? Pour en savoir davantage sur la protection, veuillez consulter la Partie D : Protection efficace en matière de sécurité, ainsi que la Question 14 qui porte sur la défense en profondeur.	
Détecter	Détecter est la troisième couche de la stratégie de cybersécurité du NIST. Cette couche est comparable à une stratégie de sécurité pour la maison. Si la couche Protéger comporte des clôtures, des barreaux dans les fenêtres et des serrures pour les portes, la couche Détecter inclurait des caméras de sécurité, des détecteurs de mouvement et un centre de surveillance de la sécurité. Les administrateurs devraient connaître le terme « activité anormale », qui décrit des activités, effectuées par le système ou des personnes, qui sortent du cadre des comportements attendus. Les anomalies sont des éléments déclencheurs de sécurité que la direction devrait surveiller. La direction devrait mettre en place des capacités de détection qui surveillent la présence potentielle d'événements touchant la sécurité, qui déclencheront des réponses (voir la Partie E : Détection des événements de cybersécurité, pour en savoir davantage).	• Anomalies et événements • Surveillance permanente de la sécurité • Processus de détection
Répondre	Malgré tous les efforts déployés, des entorses à la sécurité sont inévitables. Lorsque ces événements se produisent, la direction doit être en mesure de répondre avec efficacité.	• Planification de la réponse • Communications • Analyse • Atténuation • Améliorations

Fonction (couche) du cadre du NIST	Définition de la fonction du cadre du NIST	Catégories du cadre du NIST (par fonction)
	Le cadre de cybersécurité du NIST prévoit que les activités de réponse de la direction doivent être coordonnées avec des parties prenantes internes et externes (p. ex. un soutien externe de la part d'organismes d'application de la loi). L'analyse des événements touchant la sécurité devrait être effectuée en vue d'informer la direction au sujet de leur nature et de leur objectif. Des activités de réponse efficaces peuvent prévenir ou limiter l'expansion d'un événement et son incidence sur l'organisation. L'apprentissage continu améliorera les activités de réponse de l'organisation à l'avenir (voir la Partie F : Réponse et récupération à la suite d'une intrusion).	
Reprendre	Les capacités structurées en matière de cybersécurité pour reprendre sont souvent maîtrisées en dernier lieu par les équipes de direction. Les administrateurs sont encouragés à demander à la direction des preuves indiquant que des capacités de reprise sont en place pour : • restaurer les systèmes ou les actifs touchés par des incidents de cybersécurité. Ces capacités pourraient inclure les sauvegardes de données, les applications, les réseaux, les systèmes informatiques et les systèmes opérationnels; • coordonner les activités de restauration avec les parties prenantes internes et externes (p. ex. les centres de coordination, des fournisseurs de services Internet, les centres de données, les fournisseurs de systèmes en nuage, les propriétaires de systèmes d'attaque, les victimes, d'autres équipes d'intervention en cas d'incident de sécurité informatique (CSIRT – voir le glossaire) et des fournisseurs, entre autres (voir la Partie F : Réponse et reprise après une intrusion).	• Planification de la reprise • Communications

Source : NIST.SP.1800-5, *IT Asset Management Guide*, 2018.

2. Comment le conseil doit-il s'organiser pour gouverner efficacement la cybersécurité?

Afin d'offrir une gouvernance efficace en matière de cybersécurité, un conseil doit décider de la meilleure façon de s'organiser pour cette tâche. Il y a plusieurs modèles comportant chacun des avantages et des inconvénients (voir le tableau ci-dessous).

Dans tous les cas, il incombe au conseil d'inclure la cybersécurité à titre de compétence essentielle dans la matrice des compétences du conseil, et de nommer des personnes au conseil en conséquence. Il est conseillé de répartir la gamme de cybercompétences entre plusieurs administrateurs plutôt que de se fier à une seule personne pour interpréter les rapports de cybersécurité.

Direction de la cybergouvernance	Avantages	Inconvénients	Conclusion
Cybergouvernance dirigée par le comité d'audit	• Esprit d'analyse • Approche de type « faire confiance, mais vérifier » • Expérience connexe en audit informatique	• Peut tendre vers une approche axée sur la conformité • Est susceptible de posséder moins de compétences techniques pertinentes	Possible
Cybergouvernance dirigée par le comité des risques	• Perspective fondée sur les risques • Expérience connexe en gouvernance des risques liés aux TI	• Les cyber-risques constituent un seul des nombreux types de risques examinés	Favorable
Cybergouvernance dirigée par le comité de cybersécurité	• Les compé-tences de l'équipe spécialisée se traduisent par une gouvernance de qualité supérieure	• Il n'est pas réaliste de créer un sous-comité pour chacun des sujets de gouvernance	Favorable
Cybergouvernance dirigée par le conseil d'administration au complet	• Au courant des principaux cyberrisques et des initiatives connexes • Large éventail de questions et de points de vue	• Trop de personnes pour la gouvernance • Manque possible de compétences minimales pour gouverner de manière responsable	Possible

Bien qu'aucun modèle de gouvernance ne s'applique à tous les conseils d'administration, une combinaison des scénarios ci-dessus peut constituer une bonne solution pour nombre de conseils.

Recommandation : Attribuer la responsabilité de la cybersécurité à un comité des risques. Des tableaux de bord contenant des indicateurs récurrents (voir la Partie G) pourraient être remis tous les trois mois, avec des présentations semestrielles, à l'ensemble du conseil d'administration.

3. Comment la direction procède-t-elle pour identifier, évaluer et hiérarchiser les risques en matière de cybersécurité et pour faire rapport sur ces risques?

Comment un conseil d'administration peut-il interagir efficacement avec la direction au sujet des risques liés à la cybersécurité? Pour que ce soit possible, la direction doit appliquer un processus bien conçu de gestion des cyberrisques. Tout en évitant d'être trop directifs, les administrateurs sont encouragés à rechercher les éléments suivants dans un programme efficace de gestion des risques liés à la cybersécurité.

- Un programme solide en matière de risques liés à la cybersécurité commence par un résumé des priorités stratégiques de l'organisation (objectifs, processus et actifs de l'entreprise).
- Le programme devrait identifier les principaux cybermenaces, vulnérabilités et événements de risque potentiels qui auraient une incidence négative sur les priorités de l'organisation.
- Tout comme dans le cadre des programmes de gestion du risque d'entreprise (GRE), les événements de risque lié à la cybersécurité sont identifiés, puis évalués selon des critères d'incidence et de probabilité.
- La direction devrait établir des cibles pour les risques (à l'aide des mêmes échelles d'incidence et de probabilité) afin de confirmer le niveau de risque acceptable pour chaque événement de risque potentiel.
- La direction devrait fournir un plan de réponse en cas de risques liés à la cybersécurité qui identifie les contrôles et les autres mesures nécessaires en vue de rapprocher chaque risque du niveau ciblé.
- La responsabilité de chacun des événements de risque liés à la cybersécurité devrait être assignée à une personne précise qui devra rendre des comptes à cet égard. La mise en œuvre des contrôles peut incomber ou non à cette personne, mais elle conserve en dernier ressort l'obligation de rendre des comptes à l'égard des contrôles en place, qui doivent être efficaces et fonctionner comme prévu.
- La direction devrait créer et remplir un registre des risques liés à la cybersécurité en vue d'y consigner l'ensemble des informations pertinentes concernant son programme, notamment les événements de risque, les cotes d'évaluation, les cotes cibles pour les risques, les contrôles connexes pour les événements de risque et les commentaires formulés.

Une évaluation des risques liés à la cybersécurité bien organisée permettra à la direction de créer un modèle opératoire de la cybersécurité fondé sur le classement des principaux risques par ordre de priorité. Cela se traduira par un plan d'exécution prioritaire avec une feuille de route, un plan d'affectation des ressources et un budget pour atteindre les objectifs du modèle opératoire de la cybersécurité.

4. Quel programme de formation et de sensibilisation à la cybersécurité est en place?

Bon nombre d'atteintes à la cybersécurité sont causées par des employés qui cliquent sur des liens malveillants dans des courriels d'hameçonnage. Bien que certaines attaques par hameçonnage soient très difficiles à détecter, un personnel sensibilisé qui est à l'affût des courriels suspects réduira considérablement ce risque. Comme il est peu probable que ce risque soit éliminé, la formation continue sur les techniques de cyberattaque constitue un contrôle essentiel pour toute organisation qui a recours au courrier électronique pour ses communications.

Les principales parties prenantes qui devraient recevoir de la formation sur la cybersécurité sont les suivantes :

- le conseil d'administration;
- la direction et le personnel;
- les tiers ayant accès aux systèmes de l'organisation (travailleurs indépendants, consultants, fournisseurs, partenaires, etc.).

Remarque : Il faut sensibiliser les clients afin qu'ils soient en mesure d'éviter des cyber-escroqueries pouvant les amener à révéler des données confidentielles qui exposeraient l'organisation à des pertes découlant de fraudes.

La direction peut recourir aux moyens suivants pour la formation en matière de cybersécurité :

- des webinaires;
- des présentations en personne;
- des tests en ligne;
- des affiches et des messages aux postes de travail et sur le lieu de travail;
- des écrans de veille et des rappels à l'écran;
- des tests de simulation d'attaque (par exemple, des campagnes de simulation d'hameçonnage par courriel ou par téléphone, l'appâtage au moyen de clés USB).

La fréquence de la formation et des tests devrait être proportionnelle au risque d'attaque. Ainsi, la formation sera dispensée à une plus grande fréquence dans les entreprises de services financiers ou de commerce de détail que dans les organisations dont le personnel travaille moins en réseau.

Remarque : Le pourcentage d'employés (et de membres du conseil d'administration) qui sont tombés dans le piège d'une cyberattaque simulée dans le cadre d'un exercice de formation constitue un important indicateur de cybersécurité qu'il est recommandé d'inclure dans les rapports à l'intention du conseil d'administration. La cible est de 0 %!

5. Comment la direction établit-elle une culture efficace en matière de cybersécurité?

Selon l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), « la notion de culture de cybersécurité renvoie aux connaissances, aux croyances, aux perceptions, aux attitudes, aux hypothèses, aux normes et aux valeurs des gens concernant la cybersécurité et à la manière dont elles se manifestent dans leur comportement face aux technologies de l'information[1] » [TRADUCTION]. L'établissement d'une culture de cybersécurité efficace peut malheureusement se révéler plus difficile que la mise en œuvre de la plateforme logicielle de sécurité la plus complexe. Les équipes de direction font face à de nombreux défis alors qu'elles tentent d'atteindre cet objectif :

- Le fait de prendre la cybersécurité pour un « enjeu informatique » masque le rôle que doit jouer chaque employé au chapitre de la sécurité;
- La capacité de transposer des sujets complexes de sécurité en messages assimilables est une compétence qui se trouve encore souvent à l'étape de développement dans les organisations;
- Le fait de privilégier la commodité au détriment de la sécurité peut parfois retarder l'adoption culturelle.

Les administrateurs jouent un rôle important pour favoriser la culture de cybersécurité. Ils devraient indiquer à la direction :

- de préciser à quoi devrait ressembler la culture de cybersécurité ciblée, afin que la vision finale mobilise tous les niveaux et tous les services (voir la Question 4 sur la formation);
- de démontrer comment les administrateurs renforcent la culture de cybersécurité au moyen d'une approche descendante;
- de présenter un programme de formation en cybersécurité qui contribuera à l'établissement d'une culture efficace pour les équipes des TI et des TO;
- de préciser comment la direction récompense les bons comportements en matière de cybersécurité, notamment le signalement des courriels potentiellement malveillants avant de les ouvrir.

1 *Cyber Security Culture in organisations*, novembre 2017 (www.enisa.europa.eu/publications/cyber-security-culture-in-organisations/at_download/fullReport).

Sommes-nous en sécurité?
Les administrateurs pourraient être enclins à s'informer auprès de la direction de l'état des programmes de sécurité. Bien qu'il soit légitime de s'interroger à cet égard, les administrateurs devraient éviter de poser la question : « Sommes-nous en sécurité? » En effet, cette question laisse entendre que la sécurité est un projet pour lequel il existe un point d'achèvement, alors que, en fait, la cybersécurité est un processus continu qui doit être examiné et amélioré en permanence. Des changements tant externes – comme l'apparition de nouveaux agents de menace et l'évolution des techniques d'attaque – qu'internes – comme les changements dans les environnements des TI et des TO – mettront à jour de nouvelles vulnérabilités à prendre en considération.

De plus, même les organisations qui font preuve de la plus grande diligence seront toujours exposées à des risques dans une certaine mesure. Il est tout simplement impossible de créer un niveau absolu de sécurité.

C'est pourquoi les administrateurs sont encouragés à remplacer cette question par la suivante : « Dans quelle mesure nous rapprochons-nous des niveaux ciblés de réduction des risques liés à la cybersécurité? » Cela donnera lieu à des discussions sur la sécurité plus productives et fondées sur les risques.

6. Quelles sont les obligations de conformité de l'organisation en matière de cybersécurité et leurs conséquences dans tous les pays pertinents?

Les obligations de conformité en matière de cybersécurité diffèrent selon les secteurs et les régions, et au fil du temps, raison pour laquelle il ne serait pas réaliste d'aborder toutes les normes de conformité dans cette publication. Voici plutôt une série de questions importantes que les administrateurs devraient poser à la direction au sujet des obligations de conformité de leur organisation en matière de cybersécurité :

- La direction comprend-elle bien l'ensemble des obligations de conformité en matière de cybersécurité que l'organisation doit respecter?
- Les normes de conformité sont-elles davantage directives ou fondées sur des principes (c.-à-d. qu'elles nécessitent une interprétation), ou sont-elles prescriptives?
- Quelles sont les amendes et les pénalités en cas de non-conformité?
- Quels sont les efforts et les coûts requis pour l'atteinte de la conformité comparativement au maintien de la conformité?
- Une fois les obligations de conformité respectées, nos risques seront-ils ramenés à des niveaux acceptables, ou des efforts et des coûts supplémentaires seront-ils nécessaires? Dans le deuxième cas, que faudra-t-il faire, à l'égard de quoi faudra-t-il le faire, et quels en seront les coûts?

- La direction a-t-elle conçu une fonction interne responsable du maintien de la conformité en matière de cybersécurité?
- Quelles sont les principales normes auxquelles l'organisation doit se conformer, quelles sont les dates clés à retenir, et comment la direction effectue-t-elle un suivi pour s'assurer de la conformité à la date limite stipulée?
- Comment la direction amorcera-t-elle la discussion avec les autorités de réglementation en cas de non-conformité?

Les exemples qui suivent donnent des indications sur la manière dont les normes actuelles exigent de satisfaire aux obligations de conformité.

Exemples d'obligations de conformité en matière de cybersécurité

- Identifier les actifs essentiels en matière de cybersécurité qui sont susceptibles d'être compromis (classés par ordre de risque).
- Établir une norme minimale pour les contrôles de gestion de la sécurité.
- Former le personnel (y compris les employés, les travailleurs indépendants et les fournisseurs) ayant un certain niveau d'accès aux systèmes essentiels.
- Maintenir une sensibilisation générale à la cybersécurité pour tous les employés.
- Mettre en place des périmètres et des moyens de dissuasion tant électroniques que physiques pour les actifs essentiels en matière de cybersécurité.
- Limiter l'accès aux systèmes et aux données aux personnes dont le rôle exige un tel accès.
- Établir des plans de réponse et de reprise, et en répéter l'exécution.
- Demander des notifications obligatoires pour les parties prenantes touchées par une intrusion.
- Établir et maintenir des exigences minimales pour le chiffrement des données.
- Maintenir la confidentialité, l'intégrité et la disponibilité des données et des systèmes.
- Déterminer des durées de conservation minimales et maximales avant de pouvoir détruire des données en toute sécurité.
- Demander des historiques d'audit obligatoires.

Des évaluations des obligations de conformité de l'organisation en matière de cybersécurité effectuées par des tiers, en ayant recours à des auditeurs externes et internes et à d'autres fournisseurs de services de certification, procureront au conseil d'administration un rassurement additionnel quant au respect des obligations dans chacun des pays concernés (voir également la Question 7).

7. Comment la direction établit-elle une assurance indépendante quant à la conception et à l'efficacité de son programme et de ses contrôles en matière de cybersécurité?

Évaluations de cadres de cybersécurité établis

Tout comme pour les autres secteurs de certification, la direction a intérêt à demander des évaluations indépendantes faisant appel à des normes de cybersécurité établies. Les avantages évidents de ces examens comprennent une assurance à l'égard des degrés de maturité et des contrôles actuels en matière de sécurité, ainsi que la réception de recommandations visant à améliorer la gestion des risques liés à la sécurité et la performance.

Audits

L'audit interne convient bien pour auditer systématiquement la cybersécurité par rapport aux politiques, aux procédures ou aux obligations de conformité. Un audit externe des contrôles généraux informatiques (CGI), qui ne s'applique pas uniquement aux systèmes financiers, aux composantes, aux processus et aux données de l'environnement informatique d'une organisation, constitue une autre source d'évaluation indépendante. Toutefois, pour remettre en question l'organisation au-delà des audits courants, les aspects suivants devraient aussi être intégrés aux cycles d'audit pluriannuels :

- la conformité de l'entreprise aux politiques et procédures internes en matière de cybersécurité;
- les processus de réponse aux incidents de sécurité;
- la sécurité physique des cyberactifs;
- la conformité aux programmes obligatoires de formation en cybersécurité à l'intention des utilisateurs;
- l'accès non autorisé ou mal configuré à des appareils qui contiennent ou traitent des informations sensibles;
- l'application de correctifs en temps opportun aux applications, aux systèmes d'exploitation et aux autres micrologiciels.

Test d'intrusion par un tiers

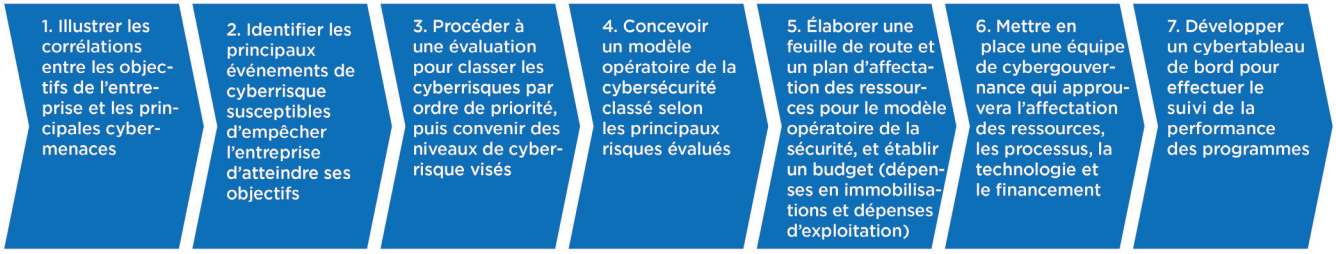
Un test d'intrusion est une simulation, autorisée par l'organisation, de tentative de piratage des applications, des systèmes informatiques, des appareils numériques et/ou des réseaux. Il a pour but d'évaluer la sécurité de l'environnement ciblé, de détecter des vulnérabilités dans cet environnement et d'évaluer les capacités de réponse et de reprise des systèmes et des équipes de sécurité de la direction.

Voici quelques renseignements importants dont les administrateurs doivent tenir compte lorsque les résultats d'un test d'intrusion leur sont présentés :

- Un test d'intrusion représente la sécurité à un moment précis. Si les systèmes de sécurité ou les techniques d'attaque changent, la validité du test d'intrusion peut diminuer.
- L'exécution d'un test d'intrusion à l'égard d'une organisation est similaire à l'exécution d'un essai d'étanchéité à l'égard d'un bateau. Si le bateau est mis à l'eau sans que la coque soit en bon état, l'eau envahira le bateau. De même, l'exécution d'un test d'intrusion à l'égard d'un système ou d'un environnement, lorsqu'on sait que la sécurité n'a pas atteint le degré de maturité requis, ne constitue pas une bonne utilisation des fonds destinés à la sécurité. En effet, il est pratiquement assuré qu'une intrusion sera détectée.
- Lorsque vous examinez les résultats d'un test d'intrusion, vous devez déterminer si les intrusions ont été effectuées uniquement au moyen d'une compromission technique ou si elles l'ont été en incitant une personne à cliquer sur un lien malveillant dans un courriel. Le premier cas reflète un problème de contrôle technique, alors que le deuxième reflète un problème de formation et de culture.

8. Comment la direction détermine-t-elle si le budget et les ressources qu'elle affecte à ces aspects sont appropriés pour gérer efficacement les cyberrisques?

Bien que la cybersécurité semble souvent être un sujet technique complexe, les administrateurs peuvent trouver rassurant le fait que la planification et l'exécution d'un programme de cybersécurité soient très similaires à la planification stratégique effectuée relativement à d'autres aspects de l'organisation. Les administrateurs devraient vérifier si la direction suit les étapes ci-dessous dans le cadre de l'élaboration d'un plan et d'un budget pour les activités liées à la cybersécurité :



Voici, à l'intention des administrateurs, un certain nombre d'informations et du contexte relativement à ce processus :

1. La principale raison d'être des programmes de cybersécurité consiste à protéger l'organisation et à accroître la probabilité qu'elle atteigne ses objectifs.
2. Les cyberrisques encourus par l'organisation sont une combinaison de menaces dirigées contre les vulnérabilités en la présence ou en l'absence d'une culture et de contrôles efficaces. Si la direction évalue plus de 25 types d'événements de cyberrisque, alors un examen du processus d'évaluation des cyberrisques s'impose.
3. Le processus d'évaluation des cyberrisques doit s'aligner sur la méthode d'évaluation de la gestion du risque d'entreprise (GRE) de l'organisation (par exemple, incidence et probabilité).
4. Un programme de cybersécurité doit être conçu en fonction des risques évalués précédemment. Il en découle un cyberprogramme fondé sur une approche descendante et sur la connaissance des risques. L'absence d'évaluation des risques entraîne énéralement une conception ascendante dans laquelle l'ordre de priorité des efforts et des dépenses peut être absent.
5. Tout comme au point 4, les feuilles de route de cybersécurité doivent être déclinées en fonction des risques. Les risques les plus élevés seront traités avant les risques plus faibles. Bien que cela semble très logique, les plans fondés sur les risques constituent toujours une nouveauté pour bon nombre d'équipes de cybersécurité.
6. Des équipes de cybergouvernance interfonctionnelles représenteront efficacement le large éventail de disciplines au sein d'une organisation.
7. Les conseils d'administration devraient mettre l'accent sur la présentation d'un ensemble de mesures répétitives (voir la Question 20).

Voici une liste non exhaustive de normes de référence générales :

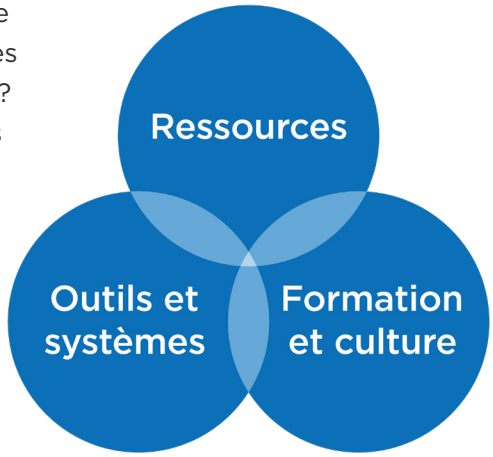
- **Cadre de cybersécurité du National Institute of Standards and Technology (NIST)** (voir la Question 1 pour un aperçu) : cadre convenant aux entreprises de toutes les tailles et de tous les secteurs d'activité;
- **Critères de description de l'AICPA énoncés dans le document intitulé *Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program*** et critères relatifs aux services de confiance énoncés dans le chapitre 100 des TSP, « 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy »[1];
- **ISO/IEC 27001 et 27002 :** normes convenant aux entreprises de toutes les tailles et de tous les secteurs d'activité;
- **Cadre COBIT (Control Objectives for Information and related Technology) :** cadre élaboré par l'ISACA, organisation mondiale qui se concentre sur la gouvernance des TI, et convenant aux moyennes et grandes entreprises de la plupart des secteurs d'activité;
- **Contrôles de sécurité essentiels (Critical Security Controls, ou CSC) du Centre for Internet Security (CIS) :** ensemble recommandé de mesures de cyberdéfense qui fournit à la direction des manières spécifiques d'atténuer les attaques les plus généralisées et dangereuses;
- **Norme de bonne pratique (Standard of Good Practice) de l'Information Security Forum (ISF) :** en provenance de l'Europe, l'ISF a établi un service central d'analyse comparative dans le cadre de sa norme (frais d'adhésion requis), qui convient aux entreprises de toutes les tailles et de tous les secteurs d'activité;
- **ANSI/ISA 62443 (anciennement ISA-99) :** série de normes et de rapports axés sur l'implantation de systèmes de contrôle et d'automatisation industrielle électroniquement sécurisés;
- **IASME Governance :** norme provenant du Royaume-Uni qui a trait à la certification de l'information pour des entreprises de petite et moyenne taille et qui permet d'obtenir une accréditation similaire à ISO 27001 avec une complexité moindre.

Remarque : Les normes spécifiques à des secteurs uniques sont trop nombreuses pour être énumérées dans cette publication.

1 Voir le site **www.aicpa.org/cybersecurityriskmanagement** ou le guide de CPA Canada intitulé ***Faire rapport sur le programme de gestion des risques d'une entité en matière de cybersécurité***.

Lors de l'examen des budgets de cybersécurité, les administrateurs doivent se préoccuper de rechercher la bonne combinaison de facteurs.

1. La direction embauche-t-elle sur une base permanente ou contractuelle une quantité appropriée de ressources compétentes pour mettre à exécution le plan proposé?
2. La direction fournit-elle à l'équipe de cybersécurité les technologies, les outils et les systèmes dont elle a besoin pour être efficace?
3. Les responsables en matière de cybersécurité ont-ils reçu l'autorité appropriée pour s'acquitter de leur rôle avec efficacité?
4. La direction a-t-elle fourni une formation adéquate pouvant raisonnablement empêcher les employés et les travailleurs indépendants d'exposer involontairement l'organisation à des attaques?



Il est maintenant nécessaire de collaborer avec les autres pour assurer l'efficacité des programmes de cybersécurité. Certains groupes sectoriels échangent des informations sur les événements de cybersécurité, des tendances, des conseils, etc. Dans ce contexte, des questions sont posées concernant le montant des budgets consacrés aux charges de fonctionnement et aux programmes d'investissement. Demandez à la direction de vous faire part des renseignements obtenus dans le cadre de ces échanges. Si elle n'y participe pas, découvrez-en la raison.

Finalement, des agences de cyberrecherche telles que Forrester ont publié des rapports et des études pour guider la direction et le conseil d'administration en ce qui a trait aux normes sectorielles. Si une société vient tout juste d'entamer son parcours en matière de cybersécurité, les dépenses pourraient être plus élevées que ce qu'indique le tableau qui suit.

VENTILATION DU BUDGET DES TI / BUDGET DU SERVICE QUI SERA CONSACRÉ À LA SÉCURITÉ EN 2008
(PAR SECTEUR)

% du budget consacré à la sécurité	Fabrication	Com merce de détail et de gros	Services à l'enter prise et construction	Services publics et télécommu nications	Services financier at assu rance	Secteur public et soins de santé
De 0% à 10%	25 %	9 %	16 %	18 %	31 %	31 %
De 11% à 20%	33 %	40 %	26 %	38 %	31 %	29 %
De 21% à 30%	18 %	19 %	23 %	32 %	20 %	21 %
Autre	23 %	33 %	35 %	12 %	18 %	19 %

Base : De 34 à 103 décideurs en technologie de sécurité globale occupant in poste de directeur on de vice-président ou relevant du chef de l'information (la taille de la base varie selon le secteur)

Source : Sondage sur la sécurité, Forrester Analytics Global Business Technographics®, 2018

PARTIE B

Cyberpirates, motifs et techniques

9. Qui (et quel type de cyberpirate) est le plus susceptible de réussir une intrusion dans l'organisation, et pourquoi?

En ce qui concerne les acteurs à l'origine des menaces, les conseils devraient comprendre :

- quels sont les acteurs à l'origine des menaces auxquels l'organisation est confrontée;

	Ennemi	Motifs	Cibles	Incidence	Vecteurs de menace
Ensemble des menaces externes	État-nation	• Avantage économique, politique et/ou militaire • Concurrence mondiale • Sécurité nationale • Fraude	• Secrets commerciaux • Renseignements commerciaux sensibles • Technologies émergentes • Infrastructure essentielle	• Perte d'un avantage concurrentiel • Perturbation de l'infrastructure essentielle • Perte de propriété intellectuelle • Perte monétaire	• Cybercampagnes à long terme, ciblées, avec une orientation stratégique • Faiblesse / manque de connaissances d'une personne en interne • Tiers fournisseurs de services
	Cyber-criminels	• Gains financiers immédiats • Collecte d'informations pour de futurs gains financiers • Fraude • Vol d'identité	• Système financier / de paiement • Renseignements permettant d'identifier une personne • Informations relatives aux cartes de paiement • Renseignements protégés sur la santé • Propriété intellectuelle	• Demandes d'informations de la part des autorités de réglementation et pénalités • Poursuites intentées par des consommateurs/actionnaires • Atteinte à la réputation et dommages financiers • Atteinte à la sécurité des données • Perte de propriété intellectuelle	• Cybercampagnes ciblées • Faiblesse / manque de connaissances d'une personne en interne • Tiers fournisseurs de services
	Cyber-terroristes	• Changement politique et/ou idéologique • Création de sentiments de peur, d'incertitude et de doute • Chaos malveillant	• Infrastructure essentielle • Technologies opérationnelles • Sites hautement visibles	• Déstabilisation, perturbation et destruction d'actifs physiques et logiques	• Vulnérabilités opportunistes • Faiblesse / manque de connaissances d'une personne en interne • Tiers fournisseurs de services
	Cyber-militants	• Influencer le changement politique et/ou social • Exercer des pressions sur les entreprises pour qu'elles changent leurs pratiques	• Secrets d'entreprise • Renseignements commerciaux sensibles • Informations relatives aux principaux cadres, aux employés, aux clients et aux partenaires d'affaires	• Perturbation des activités commerciales • Atteinte à la marque et à la réputation • Perte de la confiance des consommateurs	• Organisations ciblées qui s'opposent à leur cause • Faiblesse / manque de connaissances d'une personne en interne • Tiers fournisseurs de services
Ensemble des menaces internes	Personnes en interne	• Avantage personnel, gain financier • Vengeance professionnelle • Patriotisme	• Ventes, ententes, stratégies de marché • Secrets d'entreprise, propriété intellectuelle, recherche et développement • Activités de l'entreprise • Renseignements personnels	• Divulgation des secrets commerciaux • Perturbation des activités • Atteinte à la marque et à la réputation	• Accès préautorisé • Connaissances privilégiées

- ce que fait ou possède l'organisation qui est susceptible d'intéresser les acteurs à l'origine des menaces;
- toutes les mesures prises par la direction pour atténuer le risque que se répètent des menaces déjà perpétrées contre la société ou son secteur d'activité;
- si la direction se tient au courant des cybermenaces actuelles en lisant des rapports de veille stratégique pouvant être mis en œuvre;
- que la direction fournit régulièrement des documents d'information significatifs sur les cybermenaces et sur la sensibilisation aux questions qui s'y rapportent.

10. De quelle façon l'organisation est-elle susceptible de faire l'objet d'une intrusion?

Avant de comprendre de quelle façon l'organisation est susceptible de faire l'objet d'une intrusion, la direction doit d'abord comprendre l'environnement. Le fait de comprendre ce qui est le plus important pour l'atteinte des buts et des objectifs stratégiques de l'organisation permettra la prise de décisions éclairées en matière de cybersécurité. Une évaluation des risques mettra en lumière les forces et les vulnérabilités des contrôles de cybersécurité. Cette évaluation indiquera au conseil de quelle façon l'organisation pourrait faire l'objet d'une intrusion, la probabilité qu'une telle intrusion survienne et l'incidence qu'elle pourrait avoir.

Par-dessus tout, en comprenant de quelle façon l'organisation pourrait faire l'objet d'une intrusion, le conseil peut décider où investir des ressources financières et autres en vue d'atténuer les menaces actuelles et nouvelles.

Une organisation peut subir une intrusion de nombreuses façons, et la section suivante donne des conseils sur la manière de gérer ces risques. Les menaces peuvent provenir d'un tiers ou d'un fournisseur, être internes ou (selon le secteur d'activité de l'organisation) émaner d'une organisation cybercriminelle ou d'un État-nation.

Les conseils d'administration devraient vérifier si, dans le but d'atténuer l'incidence d'une intrusion, la direction :

- a effectué une évaluation des risques pour obtenir des informations concernant les contrôles de cybersécurité en place et les lacunes potentielles des défenses;
- a vérifié si les outils et les processus nécessaires sont en place pour accroître la visibilité de l'environnement de l'organisation, et si la direction comprend l'ensemble des menaces pour l'organisation;
- a effectué un exercice de modélisation des menaces sur la base des résultats de l'évaluation des risques et de l'analyse de l'ensemble des menaces, de manière à simuler de quelle façon l'organisation pourrait faire l'objet d'une intrusion.

Remarque : Une évaluation des risques est un instantané de la situation pris à un moment précis. Elle doit être constamment mise à jour, tout comme les autres plans d'atténuation des risques.

PARTIE C

Identification de ce qui importe le plus à l'organisation et de son degré de vulnérabilité

11. Comment la direction a-t-elle défini et situé ses actifs numériques et physiques les plus précieux (ou « joyaux de la couronne ») qui pourraient être compromis par une cyberattaque?

Le cadre de cybersécurité du NIST a été élaboré en sachant qu'il est impossible de protéger tous les actifs (informations et systèmes) en tout temps et contre toutes les menaces imaginables. Les organisations ne disposeront jamais des ressources, financières ou humaines, nécessaires pour protéger la totalité de leurs actifs précieux. Par conséquent, la direction doit déterminer un classement pour les actifs, puis prendre des mesures pour les protéger à l'aide des contrôles appropriés. Les actifs les plus sensibles sont souvent appelés les « joyaux de la couronne », ce qui leur confère un statut spécial au sein de l'entreprise.

Les joyaux de la couronne les plus courants comprennent ce qui suit :

- les données personnelles relatives aux clients, aux employés, aux travailleurs indépendants et aux investisseurs actuels et passés;
- la version avant publication des informations financières, des renseignements relatifs aux fusions et acquisitions, des contrats, des accords commerciaux, des documents relatifs à des litiges et autres;
- la propriété intellectuelle, y compris les dessins, les diagrammes de réseau, les recettes, les demandes de brevet et autres;
- les technologies de l'information et les technologies opérationnelles telles que les systèmes de contrôle et d'acquisition de données (SCADA), les applications de gestion des relations avec les clients;

- tout système ou application dont la perturbation aurait une incidence considérable sur les activités;
- tout système ou application dont l'utilisation abusive ou la compromission pourrait avoir une incidence considérable au chapitre des fraudes.

Par exemple, les renseignements personnels des clients et des employés d'une organisation constituent un actif très sensible. Leur perte ou leur vol exige un avis public aux personnes concernées et, très souvent, au commissaire à la protection de la vie privée fédéral ou provincial. Une entreprise peut aussi classer ses données financières comme étant très sensibles avant leur publication. La liste de prix des produits ou des services pourrait être sensible ou non, selon la nature de l'entreprise. Plus les données sont sensibles, plus les contrôles requis doivent être serrés et restrictifs.

La question de savoir si la direction considère les courriels comme un actif sensible de la société est pour le moins incertaine. La direction devrait toutefois prendre en compte le fait que la plupart des divulgations involontaires d'informations sensibles se produisent au moyen de courriels. Il est encore plus difficile d'identifier certains des systèmes qui contrôlent le fonctionnement et l'utilisation des ressources d'information. Un joyau de la couronne peut être à la fois une ressource d'information et un système ou une application. Certains joyaux de la couronne sont également des actifs sous forme de documents, comme des contrats signés par des clients.

Les administrateurs devraient poser les questions suivantes à la direction :

- Avez-vous déterminé les critères de classement des données?
- Avez-vous spécifié les contrôles de protection requis à chaque niveau?
- Quel est l'état actuel des données les plus sensibles qui sont protégées selon le niveau requis par la politique? Par exemple, si seulement 10 % des données critiques sont protégées conformément à la politique, cela indique qu'il reste encore beaucoup de travail à accomplir pour protéger ces joyaux de la couronne.
- Un inventaire exact et à jour de ces données a-t-il été dressé, et précise-t-il notamment où et quand elles sont stockées dans des emplacements tiers, y compris le nuage? L'exactitude de cet inventaire est l'un des facteurs clés de succès pour réduire le risque que ces données soient compromises. La direction ne peut pas protéger des informations ou des actifs numériques si elle n'est pas au courant de leur présence dans son périmètre, y compris son périmètre virtuel.

Les administrateurs devraient demander à la direction de décrire les processus de rafraîchissement du classement des données, les contrôles de protection à appliquer en fonction du classement ainsi que la manière dont elle maintient un inventaire exact de ces ressources d'information. Même si le budget est limité, l'état des joyaux de la couronne doit être clair.

De façon générale, le chef des TI devrait être responsable du développement et du maintien de l'inventaire des actifs. Toutefois, peu d'organisations ont centralisé le contrôle dans une seule personne ou un seul groupe. Par exemple, le service des ressources humaines reçoit probablement les curriculum vitæ de tous les postulants. Que fait-il des curriculum vitæ qui sont inutiles pour les postes actuellement à combler? Le chef des ressources humaines est-il autant préoccupé par la cybersécurité que le chef des TI? La réduction du risque lié à la cybersécurité est un travail d'équipe.

12. Où les vulnérabilités de l'entreprise se trouvent-elles dans les environnements de TI et de TO de la société?

Dans le cadre de la surveillance de la stratégie d'une entité, les administrateurs devraient comprendre la technologie sur laquelle repose le succès de l'organisation. La technologie numérique fait disparaître les frontières traditionnelles du secteur et offre aux innovateurs davantage d'occasions d'en déloger les grands acteurs. Bien que la technologie ait par le passé été considérée comme un catalyseur des activités de l'entreprise, elle est maintenant largement reconnue comme un moteur essentiel de croissance.

Les formes traditionnelles de technologie, habituellement désignées collectivement par le terme technologies de l'information ou TI, étaient les plateformes fondamentales qui prenaient en charge les fonctions principales et administratives de la plupart des entreprises. Le chef de l'information était responsable de ces technologies.

Il existe toutefois d'autres types de technologies qui sont utilisées par les sociétés pour mettre en œuvre leur stratégie. Les technologies opérationnelles (TO) permettent la poursuite des activités de l'entreprise. Par exemple, la technologie qui contrôle le fonctionnement d'un four dans une boulangerie ou la fonderie dans une usine d'acier fait partie des TO. Le NIST définit les TO comme du matériel et des logiciels qui détectent ou causent un changement au moyen d'une surveillance directe et/ou du contrôle d'appareils physiques, de processus ou d'événements dans l'entreprise. Jusqu'à présent, les TO n'étaient pas la cible de cyberattaques, car la plupart des systèmes n'étaient pas connectés à Internet. Cette situation a considérablement changé en raison de la pression exercée sur la direction pour accroître l'efficience et réduire les coûts. Les TO étaient traditionnellement supervisées par le chef des technologies ou le chef de l'ingénierie.

Les administrateurs doivent être certains que tant les TI que les TO font partie d'un programme de cybersécurité global. Les TI et les TO sont trop souvent cloisonnées, ce qui a pour effet que le programme de cybersécurité n'est pas équivalent pour ces deux aspects. Un programme de cybersécurité pour les TI qui est parvenu à pleine maturité devient moins efficace si l'environnement des TO y est connecté avec moins de contrôles. L'organisation

pourrait même être davantage exposée au risque s'il y a des différences. Les administrateurs devraient interroger la direction au sujet de la culture de cybersécurité dans les deux groupes technologiques.

Le tableau ci-dessous illustre les formes de systèmes de TI et de TO.

EXEMPLES DE TECHNOLOGIES DE L'INFORMATION ET DE TECHNOLOGIES OPÉRATIONNELLES

Technologies de l'information (TI)	Technologies opérationnelles (TO)
• Système de courrier électronique • Système de facturation et de service à la clientèle • Système financier • Progiciel de gestion intégré • Site Web à l'intention des clients	• Caisses enregistreuses des points de vente • Système de contrôle du chauffage, de la ventilation et de la climatisation • Système de contrôle d'un four de cuisson • Réseau de vidéosurveillance • Systèmes de gestion des immeubles

La connexion d'un nombre grandissant d'appareils à Internet (c.-à-d. l'Internet des objets, ou IdO) permet de nombreuses stratégies d'entreprise. Moniteurs d'activité physique, domotique et télématique automobile : ces appareils génèrent des données qui peuvent instantanément aider à la fois le client et la société qui les ont fournies.

Toutes ces technologies sont vulnérables à des compromissions.

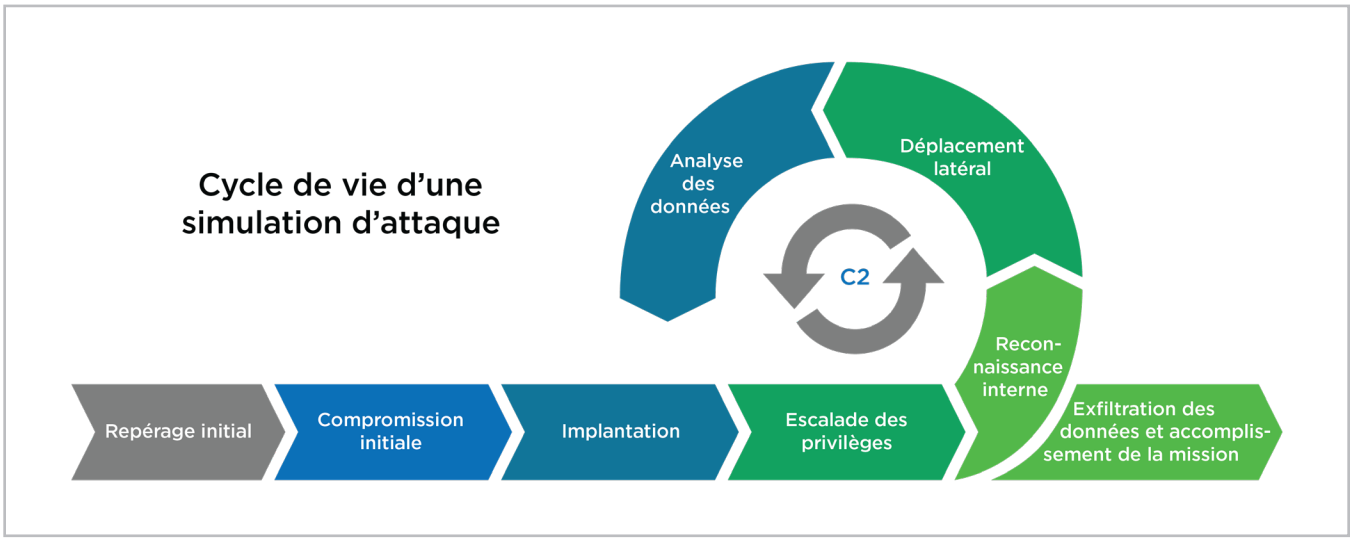
Les administrateurs doivent demander à la direction :

- d'identifier les vulnérabilités qui sont pertinentes pour l'entité et de mettre en place des mesures pour réduire la probabilité de leur survenance ou leur incidence si elles surviennent (ou encore les deux);
- de décrire les mesures prises – notamment les évaluations des risques techniques, les tests d'intrusion, les évaluations de la vulnérabilité – afin de pouvoir élaborer un plan d'action.

Les gens sont au cœur de la capacité de la direction à détecter des tentatives d'attaque et à y répondre. Par exemple, la direction pourrait recourir à une « équipe rouge » (c.-à-d. un groupe de professionnels externes hautement compétents) pour simuler une cyberattaque contre la société, afin de démontrer de quelle façon il serait possible de compromettre l'environnement. Les informations découlant de cette simulation seraient ensuite utilisées afin de mettre en place de meilleures capacités pour détecter des activités similaires et, potentiellement, réduire l'incidence d'une tentative de compromission.

SIMULATION D'UNE ATTAQUE POUR DÉTERMINER LES VULNÉRABILITÉS

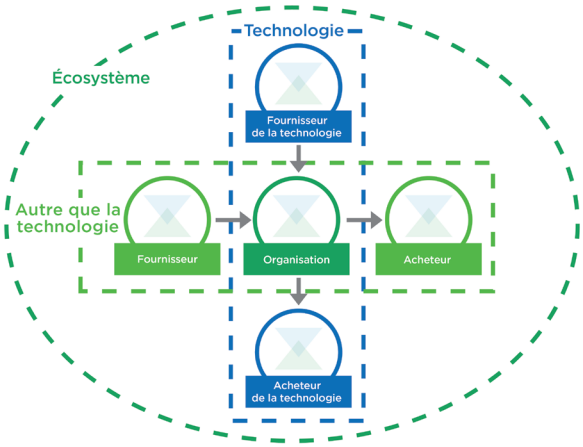
Les administrateurs devraient s'informer au sujet des évaluations entreprises par la direction, demander pourquoi ces évaluations sont suffisantes et s'enquérir des programmes recommandés, par exemple en ce qui a trait notamment à la formation, aux changements dans les



processus et aux nouvelles technologies de détection. Si les administrateurs ne sont pas à l'aise à l'idée d'évaluer les réponses de la direction aux questions qu'ils lui posent (autrement dit, à l'idée de remettre en cause les réponses de façon compétente), ils devraient recourir à des professionnels externes en cybersécurité pour obtenir un autre point de vue.

13. Comment la direction confirme-t-elle que les risques d'atteinte à la cybersécurité par des tiers (par exemple, travailleurs indépendants, fournisseurs et partenaires) sont gérés efficacement?

Le cadre de cybersécurité du NIST, mentionné plus haut, en est maintenant à la version 1.1 (avril 2018). L'un des principaux changements par rapport à la version 1.0 est l'accent mis sur l'importance de la gestion du risque lié à la chaîne logistique (voir la figure adjacente) dans le cadre de la réduction du risque lié à la cybersécurité. De nos jours, les sociétés ne fonctionnent pas entièrement par elles-mêmes.



Relations de la cyberchaîne logistique

Elles sont reliées aux clients et aux fournisseurs, elles achètent du matériel, elles vendent du matériel usagé, et elles échangent des informations avec des tiers, des autorités de réglementation et d'autres parties prenantes. La direction doit s'assurer que ses contrôles à l'égard des informations sont aussi solides, voire plus solides, lorsque ses données :

- sont en possession de ces tiers;
- sont transmises à ces tiers ou proviennent d'eux;
- ne sont plus nécessaires à ces tiers.

La direction devrait avoir mis en place trois éléments fondamentaux au sujet desquels les administrateurs devraient s'informer avant que des données ne soient échangées avec des tiers ou obtenues auprès d'eux :

1. les politiques;
2. les contrats;
3. les objectifs et les ententes sur les niveaux de service.

Des politiques devraient être rédigées et mises à jour périodiquement afin d'aider les employés et les autres principales parties prenantes à comprendre leurs responsabilités en ce qui a trait aux données. Ces politiques devraient préciser ce qu'il en est concernant l'utilisation acceptable de la technologie ainsi que la collecte, l'utilisation, la protection, le partage et la destruction des données, entre autres choses. Les politiques établissent les balises de l'organisation et servent de base pour la formation, le développement et l'acquisition de systèmes, les mesures disciplinaires et ainsi de suite. L'une de ces politiques est celle concernant la protection des renseignements personnels dans l'entreprise, qui devrait clairement décrire comment une organisation composera avec les principes généralement reconnus en matière de protection des renseignements personnels, en ce qui concerne l'utilisation des renseignements personnels.

Le principal mécanisme régissant les relations entre des entités ou des parties est un contrat commercial. Par le passé, les sociétés accordaient peu d'attention aux clauses relatives à l'échange d'informations, mais, comme le précise la version 1.1 du cadre du NIST, ces clauses sont maintenant essentielles pour réduire le cyberrisque. La direction devrait obliger par contrat les tiers à protéger les données, à participer à des exercices de résilience et à maintenir la confidentialité, l'intégrité et la disponibilité des données. Des clauses devraient également être ajoutées aux contrats existants ainsi qu'aux nouveaux contrats afin de préciser la responsabilité des tiers quant aux dommages découlant de leurs actions. Ces clauses seront difficiles à négocier avant un incident, mais impossibles à négocier après.

Le conseil d'administration devrait également retenir que l'une des modalités contractuelles clés réside dans le droit de l'entité d'auditer la conformité des tiers aux clauses de protection de l'information. Un tiers peut bien dire, par exemple, que les antécédents des membres clés

du personnel feront l'objet d'une vérification, mais il n'y aura aucune certitude que cela a réellement été fait. En outre, la plupart des tiers ne permettront pas à leurs clients d'entrer dans leurs locaux et d'observer le fonctionnement des contrôles en action.

Les sociétés utilisent les rapports sur les contrôles d'une société de services (SOC) pour montrer à leurs clients les contrôles qui sont en place et l'efficacité de leur fonctionnement sur une période donnée. La direction devra probablement se fier à ces rapports des fournisseurs clés plutôt qu'à de réels audits.

Les administrateurs doivent s'assurer :

- que des politiques conformes à la stratégie de l'entité sont en place et appliquées;
- que l'entité dispose d'une protection appropriée par le biais des contrats commerciaux;
- qu'une assurance suffisante a été obtenue indiquant que le comportement des tiers connectés est conforme à leurs obligations.

PARTIE D

Protection efficace en matière de sécurité

14. Quelle est la stratégie de « défense en profondeur » de la direction au chapitre de la combinaison de couches de protection pour les actifs les plus précieux de l'organisation?

La défense en profondeur combine de multiples couches de sécurité pour identifier les menaces potentielles et les vulnérabilités, protéger l'organisation contre des attaques internes et externes, détecter les comportements anormaux, répondre efficacement aux attaques et restaurer avec efficience les conditions de fonctionnement standards de l'organisation.

Chaque couche devrait combiner des ressources internes et externes, des logiciels et du matériel de sécurité, ainsi que des processus permettant à ces éléments de fonctionner ensemble. Il n'existe pas une combinaison unique de couches de sécurité s'appliquant à toutes les organisations. En fait, différentes configurations de sécurité peuvent être tout aussi efficaces au sein de la même organisation.

Comment alors des conseils d'administration non techniques peuvent-ils jouer un rôle de gouvernance dans cette discussion complexe? La réponse consiste à se reporter à un cadre de sécurité comme celui du NIST pour orchestrer les discussions de gouvernance. Les administrateurs peuvent utiliser les cinq éléments du cadre de cybersécurité du NIST (identifier, protéger, détecter, répondre et reprendre) comme base pour les questions de gouvernance. À titre d'exemple, consultez le tableau ci-dessous.

DÉFENSE EN PROFONDEUR

Couche de sécurité	Exemples de sécurité	Questions clés en gouvernance
Identifier	• Gouvernance • Cybermenaces et évaluations des risques • Évaluations de la vulnérabilité en matière de sécurité • Information sur les cybermenaces • Gestion des actifs	• Comment la direction identifie-t-elle les principaux risques encourus par l'organisation en matière de sécurité? • Quels aspects constituent des lacunes pour l'organisation?
Protéger	• Gestion de l'identité et des accès • Sensibilisation et formation • Sécurité des données • Sécurité des appareils et des actifs • Pare-feu • Correctifs • Campagne contre l'hameçonnage	• La direction se fie-t-elle aux résultats d'une évaluation des cyberrisques pour la conception de sa stratégie de protection? • Comment l'organisation assure-t-elle le maintien de la protection pendant des périodes de changement?
Détecter	• Surveillance de la sécurité (p. ex., SOC) • Logiciels antimaliciels • Logiciels de détection • Recherche proactive de présence malveillante dans les systèmes • Évaluations des compromissions • Analyses comportementales	• Comment la direction évalue-t-elle ses capacités de détection? • Comment la direction tire-t-elle une leçon des tentatives d'intrusion passées et apporte-t-elle des améliorations?
Répondre	• Processus et plans de réponse aux incidents • Analyse judiciaire de la sécurité • Communication des réponses (internes et externes) • Services de réponse	• La direction dispose-t-elle d'un plan de réponse éprouvé? • À quel moment le conseil doit-il jouer un rôle dans la réponse?
Reprendre	• Plans de continuité des activités • Restauration des données et des systèmes / reprise après sinistre • Systèmes redondants	• La direction a-t-elle effectivement testé les techniques de reprise? Ces techniques ont-elles connu du succès?

15. Comment la direction crée-t-elle une responsabilisation à l'égard de chaque composante du programme de sécurité?

Lorsqu'une analyse rétrospective d'un incident est effectuée, il est intéressant d'observer le comportement des participants dans la pièce et de voir s'ils se renvoient la balle, en disant par exemple « Personne ne savait au marketing que cette base de données du client était connectée à Internet », ou s'ils sont dans le déni, en disant par exemple « Personne ne m'a dit que je devais m'occuper de la vérification des antécédents criminels du gestionnaire; je ne vois pas comment j'aurais pu savoir qu'il avait un historique d'utilisation d'informations privilégiées ».

responsabilisation nom commun *féminin*
\ ʁɛs.pɔ̃.sa.bi.li.za.sjɔ̃ \

1. Action de rendre responsable, action de responsabiliser
2. (Gestion) Principe donnant plus de flexibilité à une personne tout en imposant une obligation de résultat et de justification.

En l'absence de responsabilisation, ou obligation de rendre des comptes, personne n'a l'impression que la tâche de protéger activement l'entité lui revient. Si le chef de la direction ne réattribue pas l'obligation de rendre des comptes, il sera responsable de la performance de la fonction de cybersécurité. Ce n'est pas une situation idéale, car un autre élément de l'obligation de rendre des comptes consiste à posséder la compétence requise pour s'acquitter efficacement des exigences liées à ce poste. Or les chefs de la direction ne sont pas tous compétents en la matière.

De nos jours, la plupart des organisations ont créé le poste de responsable de la sécurité de l'information. Il est de plus en plus courant que celui-ci soit la personne chargée de surveiller la planification, la mise sur pied et l'exécution des activités de cybersécurité au sein de l'entité ainsi que la délivrance des rapports connexes.

La personne dont relève le responsable de la sécurité de l'information peut également varier. Il s'agissait habituellement du responsable des TI (c.-à-d. le chef du service de l'information). Des conflits de gouvernance peuvent toutefois exister entre le responsable de la sécurité de l'information et le chef du service de l'information, et ces conflits doivent être bien compris.

Les administrateurs devraient poser les questions suivantes :

- Qui a l'obligation de rendre des comptes en matière de cybersécurité au sein de l'entité, et quelles sont les compétences et l'expérience de cette personne pour assumer ce poste de manière compétente? Cette personne est-elle facilement reconnaissable en tant que chef de la fonction de cybersécurité? Est-il nécessaire d'avoir un responsable de la sécurité de l'information, si ce poste n'existe pas?
- Comment la direction a-t-elle réglé les conflits au sein de la structure hiérarchique? Le responsable de la sécurité de l'information est-il libre de parler sans craindre de représailles?
- Qui assure la relève du titulaire de ce poste? Le personnel de sécurité expérimenté et qualifié fait souvent l'objet d'un fort recrutement. Si le responsable de la sécurité de l'information remet sa démission en donnant un préavis de deux semaines, la direction a-t-elle établi un plan de relève qui atténue le risque d'un manque de leadership?

Comme il a été mentionné auparavant, la cybersécurité n'est pas un enjeu informatique; tous les cadres et les services jouent un rôle dans la réduction du risque lié à la cybersécurité. La personne qui a l'obligation de rendre des comptes (p. ex., le responsable de la sécurité de l'information) doit prendre des mesures pour documenter les rôles et les responsabilités des principales cyberfonctions au sein de l'entité.

Les administrateurs devraient s'assurer que la direction a désigné un responsable pour les aspects clés qui suivent :

1. **Stratégie de cybersécurité**
   Il s'agit du plan, échelonné sur deux ou trois ans, qui vise à réduire la probabilité de survenance d'une cyberattaque contre les vulnérabilités de l'entité ainsi que l'incidence d'une telle cyberattaque si elle survient. Cette stratégie suivra probablement un cadre comme le cadre de cybersécurité du NIST décrit auparavant.

2. **Classement des données et inventaire des actifs (ou évaluation des joyaux de la couronne)**
   Il est impossible de protéger toutes les informations partout et en permanence. Un programme doit être en place pour identifier les données les plus importantes et la façon dont elles devraient être protégées.

3. **Évaluation continue/permanente des risques de menace**
   De nouvelles menaces apparaissent quotidiennement, qu'elles proviennent de l'extérieur ou de l'intérieur, à la suite de mesures disciplinaires prises contre un employé en difficulté qui a des privilèges d'accès considérables. Quelqu'un doit être responsable de l'identification des nouvelles menaces et de l'établissement de mesures d'atténuation appropriées. Ce travail est effectué en collaboration avec d'autres personnes pour obtenir une vision prospective.

4. **Gestion des tiers**
   La responsabilité de traiter avec les tiers qui sont connectés aux systèmes de l'entité doit être assignée à une personne. Les tiers doivent assurer la sécurité des données de l'entité. Le gestionnaire des tiers doit avoir l'autorité nécessaire pour déconnecter les tiers s'ils mettent en péril la réputation ou les données de l'entité.

5. **Planification et mise en place des réponses en cas d'incident**
   Une personne doit être responsable de la préparation de la réponse de l'entité en cas de compromission. Ce rôle peut être combiné aux fonctions de gestion de la continuité des activités ou de planification et reprise après sinistre.

6. **Formation et sensibilisation**
   Cette responsabilité prend une tout autre signification avec l'ajout de la formation en cybersécurité au programme de formation générale. Les parties prenantes suivantes doivent être prises en considération :
   a. les clients;
   b. les employés et les travailleurs indépendants;
   c. les cadres et leurs adjoints;
   d. les investisseurs et les membres du conseil d'administration;
   e. les tiers.

Une formation rehaussée devrait être dispensée aux personnes qui jouissent d'un « accès privilégié » aux systèmes et aux comptes, notamment les administrateurs principaux des TI et des TO. Il est essentiel que ces groupes demeurent conscients de leurs responsabilités de surveillance des systèmes en vue de déceler des événements étranges, comme des courriels d'hameçonnage ou de faux messages texte, afin de réduire l'exposition globale de l'entité au risque. Comme la formation est souvent la première victime de toute diminution des budgets, les administrateurs doivent demander à la direction comment ces programmes sont maintenus ou quel risque est accru.

Les administrateurs devraient également demander à la direction quelles sont les attestations obtenues par les principaux dirigeants au chapitre des programmes de cybersécurité. Une équipe de cybersécurité bien formée détiendra une série d'attestations de formation pertinentes qui témoigneront du degré de maturité plus élevé de l'organisation.

16. Comment la direction intègre-t-elle la sécurité dans le développement de nouveaux processus et systèmes?

Une gestion efficace de la sécurité commence par l'intégration, le plus tôt possible, des pratiques et des contrôles appropriés de sécurité dans l'organisation. La sécurité ne devrait pas faire l'objet d'une réflexion après coup. L'intégration peut être accomplie grâce à la mise en place des normes et des contrôles adéquatement définis de l'architecture de sécurité avant tout approvisionnement. Dans le même temps, les employés doivent être sensibilisés quant à la manière dont la sécurité favorise l'organisation. Une architecture de cybersécurité jumelée à des normes de sécurité permettra à l'organisation d'avoir un plan illustrant l'état actuel de la sécurité et l'état ciblé.

Malheureusement, le système de sécurité est trop souvent rajouté aux technologies et aux contrôles de sécurité existants. Le prix et la fonctionnalité constituent aussi trop fréquemment des critères d'évaluation d'un nouveau processus, et la sécurité est négligée ou n'est pas prise en compte.

Cette approche est sous-optimale, car elle signifie que le principe de sécurité dès la conception n'a pas été respecté. Les rajouts retardent souvent la livraison d'un projet ou d'un produit et créent la perception que la sécurité ralentit ou retarde les activités.

La sécurité devrait donc faire partie intégrante des exigences relatives à tout approvisionnement ou projet qui en est à la phase de conception et de développement. La sécurité devrait également être intégrée au processus de gestion des projets ou aux différentes étapes d'examen et d'approbation. De bonnes pratiques en matière de sécurité, comme la présence de champions de la sécurité intégrée, contribueront aussi à l'établissement de la sécurité comme

processus transparent dans toute l'organisation. Selon les activités et la culture de l'organisation, il pourrait être approprié d'intégrer dans les unités d'exploitation une ressource en sécurité décentralisée qui agirait comme la « voix » de la sécurité dans le cadre des activités quotidiennes.

Le conseil d'administration devrait poser les questions suivantes à la direction :

- L'organisation possède-t-elle une architecture de cybersécurité? Cette architecture est-elle maintenue et à jour?
- La cybersécurité fait-elle partie des exigences de tout approvisionnement ou nouveau projet?
- Les exigences en matière de sécurité pour un nouveau produit sont-elles comprises?
- Demande-t-on aux fournisseurs et aux tiers de se conformer à certaines exigences en matière de sécurité?
- Un processus est-il en place pour valider l'efficacité des contrôles de sécurité intégrés dans un produit?
- Des tests de sécurité sont-ils intégrés au processus de développement?

PARTIE E

Détection des événements de cybersécurité

17. Quels processus et outils sont en place pour alerter la direction lorsqu'une tentative d'intrusion est en cours?

L'une des manières les plus efficaces d'améliorer le profil de cybersécurité d'une société consiste à accroître sa visibilité. Pendant que la direction et le personnel opérationnel en cybersécurité s'occupent de leurs tâches quotidiennes, la technologie et la surveillance peuvent contribuer à assurer la sécurité de l'organisation. L'accroissement de la visibilité des activités de sécurité et des capacités de détection de la société se traduit par des temps de réponse plus courts pour prévenir un incident ou reprendre les activités après un incident. L'infrastructure des TI d'une organisation comporte de nombreuses composantes; la détection des événements de cybersécurité peut être accomplie par la surveillance des éléments suivants :

- les terminaux (tablettes, téléphones, ordinateurs portables, serveurs);
- le réseau des TI;
- le réseau des TO (le cas échéant).

La détermination du niveau « normal » d'achalandage informatique comme point de référence permettra d'observer les activités anormales et d'en faire le suivi. La surveillance au moyen d'un centre des opérations de sécurité permettra à la société de faire le suivi des menaces internes et externes grâce à l'enregistrement des accès non autorisés, d'un volume anormal ou du vol de données, et d'une escalade non vérifiée des privilèges. Cela peut contribuer à atténuer le risque d'une attaque interne (malveillante ou accidentelle) et aussi aider à déterminer la provenance possible d'une attaque (attribution) en vue de bloquer cette source ou d'empêcher d'autres contacts avec elle.

Un centre des opérations de sécurité devrait être considéré comme un multiplicateur de force pendant que des améliorations sont apportées à la base (c.-à-d. la normalité) par l'apprentissage machine grâce à l'information sur les cybermenaces (c.-à-d. des rapports émanant d'organisations comme le FS-ISAC et le CCTX) et par la mise au point de capteurs par le personnel même du centre des opérations de sécurité. Le centre des opérations de sécurité permet à l'organisation de détecter des intrusions potentielles en observant l'absence de conditions normales et la présence de conditions anormales, et en faisant un suivi à cet égard. Il est ainsi souvent possible de prévenir des cyberintrusions. Si une cyberintrusion se produit, elle peut être contenue plus facilement grâce à la visibilité accrue; de plus, du fait qu'il est possible d'y répondre plus rapidement, son incidence sur l'organisation se fera sentir pendant moins longtemps.

Le conseil d'administration devrait poser les questions suivantes à la direction :

- Quel type de surveillance l'organisation a-t-elle mis en place (centre des opérations de sécurité, terminaux, réseaux, etc.)?
- L'organisation utilise-t-elle des fils d'information sur les cybermenaces?
- L'organisation a-t-elle mis en place des mécanismes comme la gestion de l'identité et des accès pour empêcher des actions malveillantes?
- Existe-t-il un lien entre la surveillance et la prise de mesures par le personnel en fonction de l'information sur les cybermenaces?

PARTIE F
Réponse et reprise après une intrusion

18. La direction et le conseil sont-ils outillés pour répondre à une cyberattaque et pour permettre la reprise des activités?

La perception de la probabilité d'une cyberattaque contre l'organisation est passée de « si cela se produit » à « quand cela se produira ». Dans cette optique, il est impératif que l'organisation soit aussi bien préparée que possible à une telle éventualité. Cette préparation doit toucher l'ensemble des personnes, des processus, des technologies et des données. En ce qui concerne les processus, l'organisation devrait avoir mis en place un plan de réponse en cas d'incident et des scénarios. Le plan correspond au « quoi », et les scénarios sont le « comment ». Ainsi, le plan mis en œuvre dépendra du type de cyberattaque (interne ou externe, interruption des activités ou compromission des données).

Les rôles et les responsabilités dans le cadre de la réponse en cas d'incident devraient être documentés et bien compris, notamment les communications destinées aux parties internes et externes. Ces parties peuvent inclure les suivantes :

Communications internes	Communications externes
• Employés (touchés et non touchés) • Cadres • Conseil d'administration • Actionnaires (le cas échéant)	• Autorités de réglementation • Tiers/fournisseurs • Clients • Médias / organes d'information • Médias sociaux • Organismes d'application de la loi

Avec l'augmentation des signalements obligatoires d'atteintes à la protection des renseignements personnels, en raison de l'arrivée de règlements tels que la LPRPDE au Canada et le RGPD en Europe, un cyberincident peut déclencher la divulgation obligatoire des atteintes à la vie privée.

Éléments que le conseil devrait prendre en compte avant qu'une cyberattaque ne se produise :

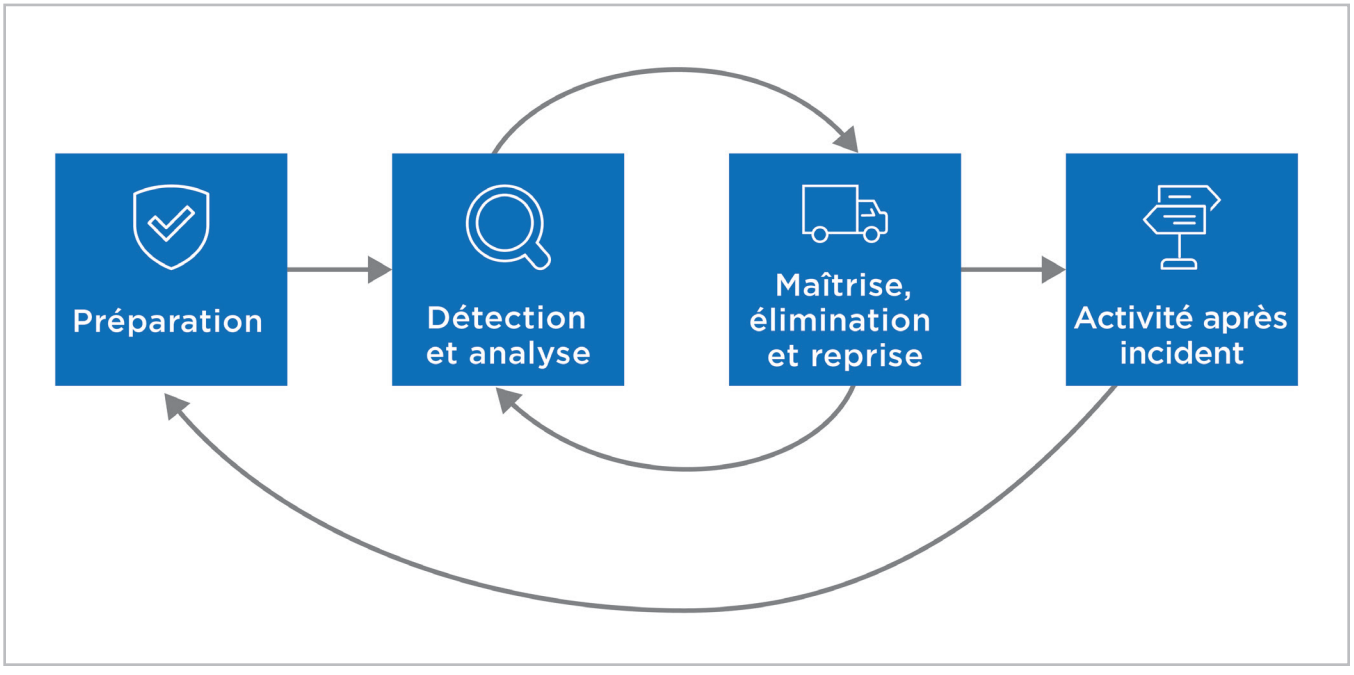
- La direction a-t-elle conçu un plan de réponse et des scénarios significatifs en cas de cyberincident?
  - Une mise à jour annuelle devrait être effectuée.
  - Cette démarche devrait être interfonctionnelle et couvrir plusieurs unités d'exploitation; une cyberattaque touche généralement les TI, la cybersécurité, les ressources humaines, les services juridiques et les communications.
- La capacité de reprise après un incident, y compris le plan et les scénarios, a-t-elle été testée au moyen de simulations d'attaque et/ou d'exercices sur table?
  - Le conseil peut y agir à titre de spectateur ou de participant, au fil de la progression de l'incident.
  - La manière la plus objective et efficace d'effectuer ces tests consiste à faire appel à un tiers. À mesure que l'organisation gagne en maturité, des tiers tels que des organismes d'application de la loi ou des fournisseurs peuvent y participer.
- La direction effectue-t-elle des sauvegardes régulièrement (pour les applications critiques, à tout le moins)? Cela permettra d'effectuer la restauration plus facilement et plus rapidement, au besoin.
- Discuter de la stratégie à appliquer en cas d'extorsion, afin de déterminer dans quelles circonstances le paiement du montant réclamé pourrait constituer une option viable dans le contexte d'un cyberincident ou d'une attaque par rançongiciel.

Éléments que le conseil devrait prendre en compte pendant une cyberattaque :

- Une équipe bien préparée et rodée consultera ou informera le conseil au sujet des éléments importants tels que les déclarations aux médias, les notifications des autorités de réglementation ou les atteintes à la réputation ou à la marque. Le plan doit être mis en œuvre et suivi, ce qui sera difficile étant donné que l'organisation sera complètement absorbée par la résolution de l'incident. L'équipe de gestion des incidents concentrera ses efforts à rétablir un niveau acceptable des activités pour l'organisation ainsi qu'à faire enquête sur l'incident et à le régler. Le plan devrait préciser des seuils de gravité et donc un ordre de priorité, ce dernier servant à définir les groupes d'unités d'exploitation qui devraient être mobilisés et le moment où ils devraient l'être. Le plan devrait également fournir des indications quant au moment où le conseil devrait être informé, ce qui, de façon générale, se produira si la marque ou la réputation sont susceptibles d'être touchées, s'il y a eu des manquements à la réglementation ou si les répercussions financières sont importantes. Le conseil devrait demander à la direction si elle a mis en place un tel processus de recours à la hiérarchie.

Éléments que le conseil devrait prendre en compte après une cyberattaque :

- Vérifier si la direction a effectué une analyse des causes fondamentales de l'attaque.
- S'assurer que des mesures correctives ont été mises en place, comme l'amélioration des contrôles, la révocation des comptes, la formation, etc.
- Vérifier si la direction a mis en place une stratégie à court, moyen et long terme pour minimiser la possibilité qu'une telle situation se reproduise.
- Intégrer les leçons tirées de l'attaque à la phase de préparation. Le processus de réponse en cas d'incident du SANS Institute, présenté ci-après, illustre les étapes que la direction devrait suivre avant, pendant et après une cyberattaque.



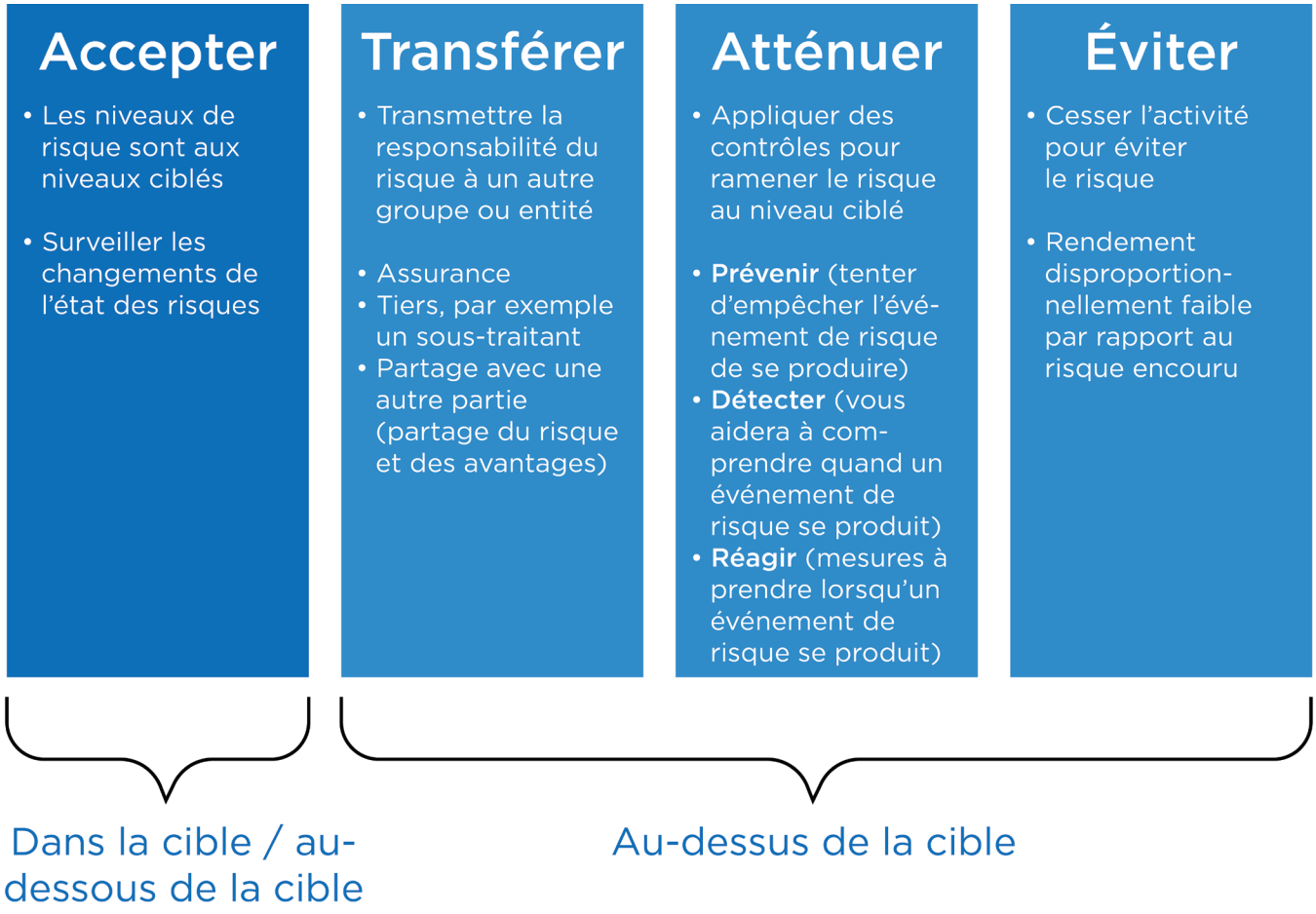
19. Quelle est la stratégie de la direction en matière de cyberassurance?

La cyberassurance est un produit émergent qui connaît une demande croissante. Elle offre de nouvelles possibilités, mais peut aussi dangereusement exposer l'organisation si elle n'est pas bien comprise ou gérée.

La cyberassurance ne réduit pas la probabilité que se produise une cyberattaque et n'aide pas une organisation à détecter ou à prévenir un cyberévénement ou incident. Elle permet cependant à l'organisation de transférer une partie du risque à un assureur. La cyberassurance donne à l'organisation un contrôle qui pourrait réduire les répercussions financières et/ou permettre la reprise des activités plus rapidement à un niveau acceptable.

La figure qui suit illustre les quatre manières de gérer le risque et indique en quoi la cyberassurance peut constituer une option pour le transfert du risque.

Comme peu de données actuarielles canadiennes sont accessibles au public en ce qui concerne les cyberattaques, il peut être difficile d'effectuer une estimation précise des primes. Des renseignements supplémentaires sont nécessaires pour intégrer des exclusions de protection. Les fournisseurs peuvent effectuer leur propre évaluation ou faire appel à un tiers objectif pour évaluer la maturité et les contrôles de l'organisation en matière de cyberrisque. Cette évaluation permettra à l'organisation de savoir quelles sont ses vulnérabilités potentielles et de mettre ensuite en place des mesures visant à améliorer la sécurité et ainsi réduire la prime.



Une façon de combler l'écart de couverture entre la cyberassurance disponible et l'assurance générale consiste à faire appel à un assureur captif. Les stratégies d'assurance captive accordent un plus grand contrôle aux sociétés, sont susceptibles de réduire le coût de l'assurance, génèrent des avantages fiscaux et améliorent les flux de trésorerie.

Le conseil d'administration devrait poser les questions suivantes à la direction :

- L'organisation a-t-elle effectué une évaluation rigoureuse des risques et envisagé la cyberassurance?
- Quelles sont les limites de la cyberassurance disponible, et comment la direction peut-elle déterminer si ces limites permettent une couverture suffisante?
- La direction a-t-elle comparé le programme de cyberassurance au profil de risque fondamental de l'organisation?
- L'organisation se conforme-t-elle à la police d'assurance?
- Est-il possible de réduire la prime en améliorant les contrôles de sécurité?
- À quelle étape d'une cyberattaque faut-il communiquer avec l'assureur?
- Toute police de cyberassurance comporte des clauses et des modalités qui doivent être respectées pour maintenir la couverture. Leur non-respect peut invalider la police ou exposer l'organisation aux risques. Vous devez comprendre ce que la direction doit faire et quels sont les risques auxquels l'organisation est exposée.

PARTIE G
Rapports

20. Comment la direction évalue-t-elle son programme de cybersécurité et fait-elle rapport au conseil à cet égard?

Aucun sujet n'aura fait l'objet d'autant de débats que la question de savoir quelles informations devraient être présentées par la direction au conseil concernant la cybersécurité, ainsi que comment et quand elles devraient l'être. Cela est dû au fait qu'aucune mesure unique ne peut fournir au conseil les informations dont il a besoin pour comprendre comment les cyberrisques sont gérés.

Un concept qui gagne en popularité est le rapport **HIFO** :

- **H**indsight (connaissances a posteriori);
- **I**nsight (points de vue);
- **F**oresight (prévisions);
- **O**versigh (surveillance).

Quelles informations sont fournies pour illustrer ce qui s'est déjà produit (connaissances a posteriori), ce qui se produira (prévisions), comment le programme de cybersécurité est géré (surveillance), et quelles informations ont une importance réelle pour les administrateurs (points de vue)?

Les administrateurs doivent également insister pour que la direction fournisse des rapports qui soient :

- **clairs :** ne pas utiliser de jargon propre à la cybersécurité;
- **concis :** utiliser des graphiques, plutôt que du texte, et d'autres techniques pour que les rapports soient plus courts et plus faciles à lire et à comprendre;
- **mémorables :** faire en sorte qu'il soit facile de se souvenir des informations et de les glisser dans des conversations avec les parties prenantes.

Les informations sectorielles doivent constituer la base du rapport. Bien qu'il puisse y avoir certains éléments communs, les besoins en matière de cybersécurité sont différents entre les secteurs bancaire et minier, entre les secteurs public et privé, et certainement entre les entreprises à but lucratif et les organismes sans but lucratif. L'étendue et la profondeur des informations à risque seront sensiblement différentes.

Connaissances a posteriori

Divers indicateurs clés de performance (ICP) peuvent être utilisés pour acquérir des connaissances a posteriori. Cela dit, il faut s'assurer que les ICP utilisés sont pertinents par rapport à ce que les membres du conseil ont vraiment besoin de comprendre. Certaines équipes de direction mettent l'accent sur le nombre d'attaques qui ont été bloquées. Ce nombre peut atteindre des dizaines, des centaines voire des milliers d'attaques. Il est beaucoup plus important toutefois de comprendre quand l'attaque a été détectée et si l'intégrité des informations a été compromise lors de l'attaque.

Prévisions

Les prévisions donnent aux administrateurs une idée de la mesure dans laquelle la société a prévu quelles personnes veulent compromettre ses données, quelles méthodes ces personnes pourraient utiliser, et quelles protections ont été mises en place pour diminuer la probabilité qu'elles parviennent à leurs fins. Les sociétés peuvent maintenant acheter de l'information de veille stratégique ou des données prospectives auprès de tiers ainsi que des renseignements sur les méthodes utilisées par ceux qui cherchent à compromettre les actifs numériques. La direction devrait également délivrer un rapport sur les tiers avec lesquels elle collabore pour obtenir des informations sur la nature des attaques qui se produisent dans son secteur. Il est souvent nécessaire de travailler conjointement avec la concurrence pour renforcer la résilience du secteur.

Surveillance

Les éléments de gouvernance sont habituellement présentés dans le volet surveillance. Ils comprennent la manière dont le programme de cybersécurité est structuré, la question de savoir si un membre de la direction qualifié et ayant l'obligation de rendre des comptes a été désigné pour remplir ce rôle et si une planification appropriée de la relève a été effectuée, ainsi que la question de savoir si le programme de cybersécurité est entièrement financé et opérationnel et s'il est axé sur les projets nécessaires pour réduire les risques futurs.

Points de vue

Enfin, les points de vue résultent de la combinaison de tous les éléments précédents pour montrer aux administrateurs que la direction agit en fonction des informations historiques, futures et opérationnelles en vue de réduire l'incidence d'une attaque de plus en plus probable des actifs numériques de l'entreprise. Dans un avenir proche, des données devront être fournies au conseil au sujet de la capacité de l'entreprise à détecter des situations anormales et de la manière dont la direction répond de façon appropriée à ces situations.

EXEMPLE DE RAPPORT DE LA DIRECTION

Fonction du cadre de cybersécurité du NIST	Faits saillants en 2017	2016*	2017	Objectif pour 2018
Identifier Mieux comprendre l'organisation en vue de gérer le risque lié à la cybersécurité en ce qui a trait aux systèmes, aux actifs, aux données et aux capacités	↗ Les politiques, les normes et les processus de gouvernance sont bien définis ↗ Les activités de gestion des risques accordent continuellement la priorité aux domaines d'investissement pour répondre aux menaces actuelles et en évolution	3,4	3,6	↗
Protéger Développer et mettre en œuvre les sauvegardes appropriées pour assurer la prestation des services essentiels liés à l'infrastructure	↗ Solides bases (p. ex., antivirus, application de correctifs) et couches de défense pour se protéger contre les menaces actuelles, comme les rançongiciels, et pour arrêter les pirates qui suivent le principe du moindre effort → Déficiences récurrentes et à faible risque du contrôle d'accès en raison de processus de certification et de révocation en temps opportun	3,4	3,5	↗
Détecter	↗ La surveillance des événements et la capacité d'exploitation sont en cours de modernisation			

Comme les administrateurs doivent souvent lire des documents comptant des centaines de pages, ils devraient insister pour que la direction effectue le dur travail de condenser les informations afin qu'elles conviennent aux administrateurs à titre de public distinct. Il n'est habituellement pas approprié que les personnes qui dirigent l'entreprise remanient des rapports de la direction qui sont significatifs pour l'exploitation de la société. Les administrateurs devraient également établir un calendrier stipulant la fréquence des rapports. De nos jours, un rapport mensuel est généralement présenté à un sous-comité du conseil d'administration, un rapport trimestriel est présenté en personne à ce même sous-comité, et une présentation annuelle a lieu devant l'ensemble du conseil d'administration. Comme il a été mentionné auparavant, le calendrier des rapports dépend du secteur (par exemple, les rapports sont plus fréquents pour les entreprises exerçant principalement des activités numériques) et de la performance de l'entreprise en matière de cybersécurité. Ainsi, une entité ayant subi un grave incident pourrait décider de faire rapport sur la performance au conseil d'administration plus fréquemment, en réponse à cet incident.

COMPTABLES
PROFESSIONNELS
AGRÉÉS
CANADA

277, RUE WELLINGTON OUEST
TORONTO (ONTARIO) CANADA M5V 3H2
TÉL. 416 977.3222 TÉLÉC. 416 977.8585
WWW.CPACANADA.CA