Gestion des risques liés à la cybersécurité

Guide pratique pour les entreprises

Table des matières

Le présent document ne contient que des renseignements généraux et n'est pas destiné à fournir des conseils juridiques. Pour obtenir de plus amples renseignements, veuillez communiquer avec l'une de nos personnes-ressources.

Risques et avantages liés à la cybersécurité

Lorsqu'il y a des données, il y a un risque de perte de données. La façon dont une organisation se prépare et gère un incident lié aux données aura un effet déterminant sur son dénouement. Un incident lié à la sécurité des données pourrait coûter des millions de dollars et détruire la réputation d'une organisation mais s'il est géré efficacement, il peut être maîtrisé et avoir une incidence considérablement moindre. À la suite d'une atteinte à la protection des données bien médiatisée mettant en cause des logiciels malveillants installés sur les bornes d'autocontrôle de Home Depot, deux entreprises canadiennes ont intenté des actions collectives pour une somme de 500 millions de dollars; les poursuites ont finalement été réglées pour 400,000 $. La réduction importante de la compensation était justifiée, a déclaré le juge, en raison de la réponse « exemplaire » de Home Depot à l'atteinte[1] :

> « Dans le cas présent étant donné que :
>
> (a) Home Depot n'a apparemment rien fait de mal;
>
> (b) elle a réagi de façon responsable, rapide, bienveillante et exemplaire aux actes criminels perpétrés contre elle par des pirates informatiques;
>
> (c) Home Depot n'avait pas besoin de gestion du comportement;
>
> (d) la probabilité de réussite des membres de l'action collective à l'encontre de Home Depot était négligeable ou faible, tant sur le plan de la responsabilité que sur celui de la preuve de dommages directs; et
>
> (e) le risque et les frais liés à l'échec du litige étaient proportionnellement substantiels et immédiats,
>
> j'aurais approuvé le désistement de l'action collective proposée par M. Lozanski avec ou sans frais et sans aucun avantage obtenu par les membres putatifs de l'action collective. »

Davantage de données

Les données sur une personne identifiable constituent des renseignements personnels. Par conséquent, la collecte de ce type de données crée des obligations en matière de protection des renseignements personnels et entraîne l'application des lois sur la protection des renseignements personnels[2]. Grâce aux progrès technologiques, les organisations recueillent, utilisent, conservent et transfèrent, plus que jamais auparavant, des renseignements personnels sur leurs consommateurs, professionnels, patients et employés. L'accumulation de vastes quantités de renseignements personnels dans de grandes bases de données augmente à la fois le risque et les conséquences potentielles de l'utilisation ou de la divulgation non autorisées de ces renseignements. En outre, les innovations technologiques récentes - comme dans le domaine de l'intelligence artificielle - permettent aux organisations d'utiliser les données de manière nouvelle et considérable. Par conséquent, un seul incident lié aux données personnelles peut maintenant toucher des millions de personnes.

Incidents de données plus importants et plus complexes

La taille et la complexité des incidents liés aux données continuent de croître. Ceci reflète la sophistication croissante des acteurs à l'origine de tels incidents. Les modèles d'affaires des auteurs ont évolué et, en plus d'utiliser des méthodes plus complexes, leurs cibles ont changé. Le *modus operandi* des auteurs d'infractions est passé

du vol de renseignements liés aux cartes de crédit à des fins d'opérations non autorisées, à des méthodes d'ingénierie sociale plus malveillantes et dommageables qui permettent l'accès aux renseignements les plus précieux d'une entreprise. Ces informations peuvent ensuite être monétisées par le biais de délits d'initiés, par la vente sur le marché noir, ou par la demande d'une rançon pour leur retour.

Pas Si mais Quand

Les préoccupations de la haute direction à l'égard d'un incident lié aux données ont augmenté de façon spectaculaire. Il est désormais entendu que les entreprises ne devraient pas demander *si* un incident lié aux données se produira, mais *quand*.

Incidents de données plus coûteux

Les incidents liés aux données sont de plus en plus coûteux. Le coût de la gestion d'un incident de données peut être considérable. Alors que de nouveaux produits, comme l'assurance contre les risques de cybersécurité, sont disponibles pour aider à couvrir les coûts, les litiges (surtout les actions collectives) représentent maintenant une réponse standard à un signalement d'incident lié aux données. Tandis que les indemnités de dommages ont varié, les organisations doivent être préparées au pire.

Les coûts ne se terminent pas avec les dommages - les incidents liés aux données peuvent entraîner la responsabilité des dirigeants et du conseil d'administration. Les cadres supérieurs se retrouvent souvent avec leur poste en péril en fonction de la façon dont ils gèrent un incident lié aux données.

Par exemple, le chef de la direction d'Equifax, Richard Smith, a démissionné à la suite de critiques en raison de l'atteinte à la protection des données de la société en 2017[3]. Le chef de l'information et le chef de la sécurité ont également démissionné[4].

Enfin, il y a des coûts réglementaires. La modification récemment proposée par le gouvernement du Québec à sa législation provinciale sur la protection des renseignements personnels prévoit des sanctions administratives pouvant atteindre 10 millions de dollars ou 2% du chiffre d'affaires mondial, selon le montant le plus élevé, et des sanctions pénales pouvant atteindre 25 millions de dollars ou 4% du chiffre d'affaires mondial[5]. En vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques* du Canada (« **LPRPDE** »), le non-respect des exigences obligatoires en matière d'avis d'une atteinte aux mesures de sécurité peut entraîner des amendes pouvant atteindre 100 000 $ par infraction[6]. Plusieurs efforts de réforme du droit de la protection des renseignements personnels sont en cours au Canada et le Commissaire à la protection de la vie privée du Canada a demandé à maintes reprises le pouvoir d'imposer des amendes[7].

De la conformité à l'avantage concurrentiel

Bien qu'auparavant la protection des données ait été considérée comme un effort de conformité difficile qui ne permettait guère d'obtenir un rendement sur l'investissement, les entreprises avisées considèrent maintenant comme un avantage concurrentiel le fait d'une meilleure protection des données et d'un solide plan d'intervention en cas d'incident. Les dépenses liées à la cybersécurité jouent un rôle stratégique et générateur de profits. Par exemple, un récent sondage de Bain & Company a révélé que les clients paieraient une prime moyenne de 22% pour de meilleures pratiques en matière de sécurité et de données[8]. De plus, l'étude de référence sur la protection des données de 2020 de Cisco, qui a mené un sondage auprès de répondants de 13 pays, dont le Canada, a révélé que plus de 40% des organisations qui investissent dans des instruments de protection des renseignements personnels obtiennent des rendements au moins deux fois supérieurs à leurs dépenses en matière de protection des renseignements personnels[9]. La perspective de telles primes devrait être un objectif clé de tout cadre en matière de cybersécurité.

02

Pourquoi la préparation à la cybersécurité est importante

Meilleurs résultats

Les 72 premières heures sont cruciales. Bien que tous les incidents liés aux données ne soient pas d'une ampleur impressionnante, la pire incursion peut plonger toute une organisation dans la tourmente pendant des mois. Les 72 premières heures qui suivent un incident de données sont, en particulier, un mélange chaotique de pièces mobiles, dont la plupart doivent être traitées simultanément, tout en s'appuyant sur des informations qui ne sont pas encore complètes.

Un plan d'intervention en cas d'incident de cybersécurité qui a été préparé à l'avance pour être mis en œuvre par une équipe d'intervention en cas d'incident formée et expérimentée contribue grandement à éviter le chaos potentiel, à maintenir les intervenants clés au courant et à concentrer les efforts de l'équipe sur les priorités établies. Il est important de noter qu'un plan d'intervention en cas d'incident permet de structurer les travaux urgents et peut constituer un frein important à l'activité non ciblée et à l'envie de « faire quelque chose ». De plus, une réponse rigoureusement réfléchie peut réduire les coûts, réduire la participation excessive des fournisseurs externes, aider à préserver les éléments de preuve qui peuvent établir que l'organisation a respecté la norme de diligence applicable, ainsi que réduire au minimum les dommages liés à la réputation.

> **Ce plan d'intervention en cas d'incident devrait s'inscrire dans le cadre d'un programme plus vaste en matière de gestion de la protection des renseignements personnels que tout organisme traitant des renseignements personnels devrait mettre en place** [10]

Évolution de la norme de diligence applicable

Un plan d'intervention en cas d'incident bien conçu, documenté et exécuté est essentiel pour limiter la perte de données et les perturbations organisationnelles. De manière encore plus importante, il peut aider à réduire la responsabilité envers les tiers et les organismes de réglementation, à condition que le plan soit régulièrement mis à jour pour tenir compte de la conscientisation aux changements liées à la cybersécurité.

Une organisation, si elle est poursuivie, peut voir ses actions et la mise en œuvre de son plan d'intervention en cas d'incident évaluées, par un tribunal. Un tribunal chargé d'évaluer le caractère raisonnable d'un plan d'intervention en cas d'incident examinera non seulement les documents écrits sur lesquels s'appuie une organisation, mais aussi, entre autres, si les politiques ont été suivies, si des ressources techniques, financières et humaines appropriées ont été allouées et si la haute direction a participé à la création et à la gestion du plan. De plus, avec l'identification de nouveaux risques et de nouvelles menaces chaque semaine, un plan d'intervention en cas d'incident ne peut être un document statique.

La norme de diligence applicable peut également être évaluée en fonction des orientations réglementaires dans des secteurs précis. Par exemple, le Bureau du surintendant des institutions financières (« **BSIF** ») a déclaré que les institutions financières sous réglementation fédérale (« **IFRF** ») « doivent réagir promptement et efficacement aux incidents liés à la technologie et à la cybersécurité »[11]. Le BSIF exige que les incidents soient signalés afin de déterminer les mesures à prendre pour « prévenir de tels incidents de façon proactive » et pour augmenter leur résilience[12].

Une approche proactive comprend des politiques, du personnel, des processus, des pratiques et des technologies utilisées appropriés pour évaluer et atténuer les risques et les attaques cybernétiques.

Bien que le BSIF n'exige pas explicitement que les IFRF aient un plan d'intervention en cas d'incident, il a néanmoins recommandé que ces plans soient élaborés et maintenus afin de se préparer adéquatement aux cyberattaques. À cet égard, en 2013, le BSIF a publié une note d' information quant aux « Conseils sur l'auto-évaluation en matière de cybersécurité » , qui prévoit que les IFRF devraient concevoir un « cadre de gestion des incidents » qui « permet de réagir rapidement aux cyberincidents importants »; « instaur[er] des procédures écrites de contrôle et d'analyse des incidents de cybersécurité et d'intervention » et qui comprennent un « processus de gestion du changement [...] [qui] permet d'intervenir promptement et de prendre des mesures d'atténuation rapides dans le cas d'incidents de cybersécurité »[13].

De même, les Autorités canadiennes en valeurs mobilières (« **ACVM** ») n'exigent pas explicitement que les membres aient un plan d'intervention en place en cas d'incident. Toutefois, dans un avis d'octobre 2017, les ACVM ont conseillé aux membres d'établir et de maintenir un plan d'intervention en cas d'incident « pour répondre à un tel incident et le signaler »[14].Les ACVM ont en outre fait remarquer que ces lignes directrices seraient prises en compte lors de l' « évalu[ation] de la façon dont les sociétés s'acquittent de leurs obligations de gestion des risques associés à leurs activités » dans le cadre des examens de la conformité[15]. Les préoccupations et les attentes en matière de cybersécurité des organismes de réglementation des valeurs mobilières, y compris les ACVM, sont abordées plus en détail dans le présent guide, à la **Satisfaire aux exigences particulières du secteur.**

Éléments clés d'un cadre

Governance

Plan de formation et de politiques

Ententes d'accès aux tiers et ententes de services de TI

Sécurité, logiciels malveillants et surveillance

Assurance contre les risques liés à la cybersécurité

03

Plan de préparation à la cybersécurité et d'intervention en cas d'incident

Bien que les incidents liés aux données soient de plus en plus fréquents, s'ils sont gérés correctement, ils peuvent s'avérer ne pas être catastrophiques. Les organisations qui intègrent la préparation aux incidents et la prévention dans leur programme global de gestion des risques de cybersécurité sont beaucoup plus susceptibles d'obtenir des résultats favorables en cas d'incident (et plus susceptibles même d'éviter un incident) que les organisations qui adoptent une approche *ad hoc*. Dans le contexte d'une atteinte à la protection des données, un « résultat plus favorable » comprend un processus de résolution d'incident qui :

- attire peu l'attention des médias;
- réduit au minimum les coûts (en particulier les coûts associés à la menace de litige);
- limite l'impact sur la réputation;
- rationalise la participation des intervenants; et
- invite les organismes de réglementation à effectuer un examen minimal.

Un **cadre de cybersécurité** est proactif. Il contient un ensemble complet de ressources organisationnelles, y compris les politiques, le personnel, les processus, les pratiques et les technologies utilisés pour évaluer et atténuer les cyberrisques et les attaques.

Un **plan d'intervention en cas d'incident de cybersécurité** est réactif. Il représente un engagement à l'échelle de l'entreprise qui fournit un protocole pour l'ensemble de l'organisation et qui attribue des responsabilités et établit des paramètres pour suivre les efforts de l'organisation pour résoudre l'incident. Il comprend une variété d'éléments spécifiques et couvre un large éventail de disciplines. Il est important de noter qu'il est complet et détaillé et qu'il ne se limite pas aux cases à cocher et aux listes de choses à faire.

Cadre de cybersécurité

Gouvernance

La cybersécurité n'est pas seulement un risque lié aux technologies de l'information. Il s'agit plutôt d'un risque à l'échelle de l'entreprise et devrait faire partie du mandat général de gestion du risque du conseil d'administration.

La cybersécurité doit être abordée aux niveaux les plus élevés de l'entreprise. La responsabilité de la cybersécurité, comme pour tout risque commercial critique, incombe en fin de compte au conseil d'administration. En cas d'incident lié aux données, les tribunaux analyseront la participation des administrateurs dans l'évaluation et l'examen des risques liés à la cybersécurité.

Dans le cas d'une poursuite intentée contre les administrateurs et les dirigeants à la suite d'un incident lié aux données, les actionnaires peuvent contester non seulement la conduite des administrateurs et des dirigeants en réponse à l'atteinte aux données, mais aussi alléguer que la conduite après la découverte de l'atteinte à la protection des données était inadéquate.

La direction et les conseils doivent être proactifs. Les points suivants représentent des étapes importantes que les dirigeants d'une organisation devraient prendre en considération lorsqu'ils déterminent et évaluent les risques de cybersécurité d'une organisation.

Mesures prises par les administrateurs et les dirigeants[16]

- Adopter des politiques, des procédures et des contrôles internes écrits en matière de cybersécurité, y compris le moment et la façon de divulguer un incident.
- Mettre en œuvre des méthodes pour détecter la survenance d'un incident de cybersécurité.
- Discuter, au niveau de la direction et du conseil, de la nomination d'un chef de l'information ou d'un chef de la sécurité de l'information ayant l'expertise pour rencontrer régulièrement et conseiller le conseil d'administration.
- Envisager de nommer un membre du conseil possédant une expertise et une expérience en cybersécurité (ou le conseil d'administration devrait consulter un expert-conseil qui pourra donner des conseils au conseil d'administration) et de nommer un comité de gestion du risque d'entreprise.
- Examiner les budgets annuels pour assurer des allocations appropriées pour les programmes de protection des renseignements personnels et de sécurité des TI.
- Recevoir régulièrement des rapports sur les incidents liés aux données et les cyberrisques.
- Comprendre clairement qui, au sein de la direction, est le principal responsable de la surveillance des risques liés à la cybersécurité et de veiller à ce que les pratiques de gestion des risques liés à la cybersécurité de l'entreprise soient adéquates.
- Déterminer quels risques doivent être abordés et atténués directement et quels risques peuvent être transférés par le biais de l'assurance.

Politiques et formation

Les politiques et procédures d'une organisation constituent un élément clé d'un programme de gestion des risques liés à la cybersécurité.

Bien que le contenu des politiques puisse varier, il existe certains éléments communs importants.

Les composantes particulières de tout programme varieront d'une organisation à l'autre, selon la juridiction, l'industrie et la tolérance au risque d'une organisation. Cependant, toutes les politiques devraient être rédigées en langage clair et être facilement accessibles (par exemple, par l'entremise de l'intranet de l'organisation). Tous les employés, quel que soit leur niveau ou leur poste, devraient être en mesure de comprendre les politiques et de recevoir une formation officielle sur la meilleure façon de s'y conformer.

Certains aspects particuliers de la formation et des politiques peuvent comprendre les considérations suivantes :

Sécurité des TI

L'organisation a-t-elle des documents et de la formation qui fournissent des lignes directrices à l'équipe de sécurité de l'information? Voici quelques éléments qu'une telle politique pourrait inclure :

- Contrôle d'accès et gestion des mots de passe.
- Gestion des connexions réseau et des pare-feu.
- Gestion des virus et des logiciels malveillants, y compris l'installation de mises à jour et de correctifs, et mécanismes de contrôle des modifications.
- Exigences en matière de chiffrement.
- Sécurité du réseau, y compris la sécurité du réseau sans fil.

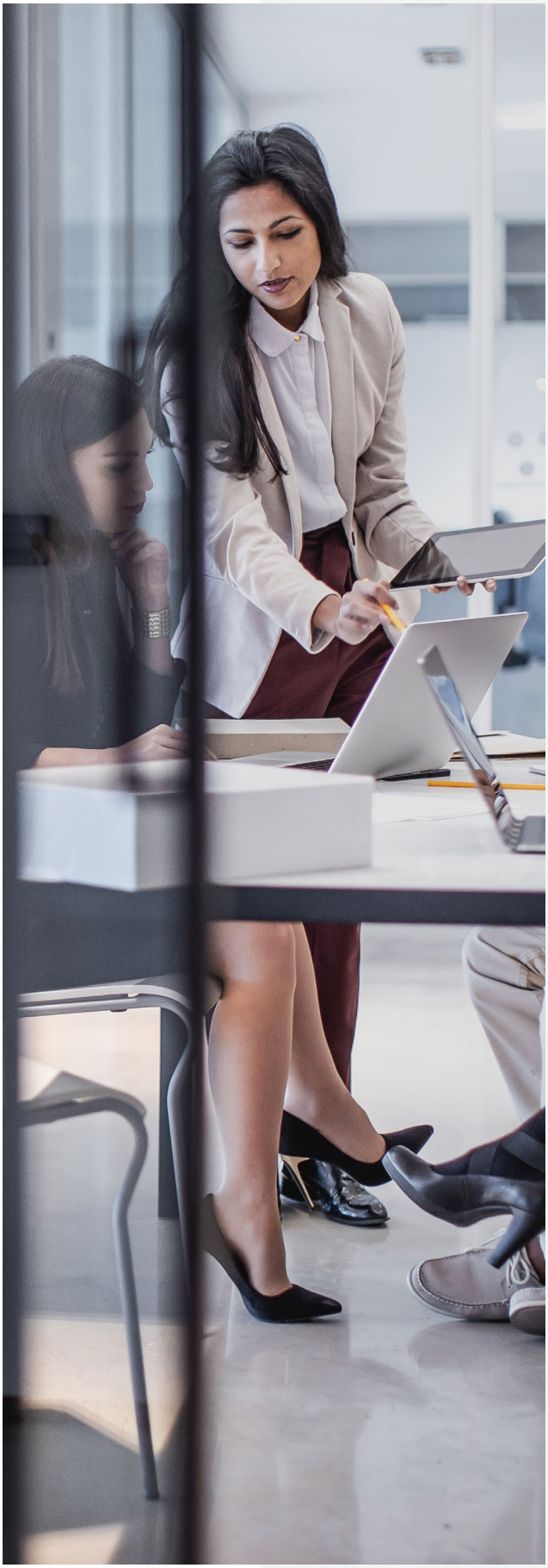
- Se préparer, réagir et remédier à un incident lié aux données, y compris un mécanisme de signalement des incidents.
- Accès à distance aux réseaux de l'organisation.
- Élimination des actifs, des périphériques et des données informatiques (y compris une politique de rétention des données).
- Maintien des opérations et reprise après sinistre.

Utilisation acceptable des actifs informatiques

- L'organisation a-t-elle des politiques en langage clair à la disposition des employés qui énoncent l'utilisation acceptable des systèmes et des actifs informatiques, des services de courriel et d'autres services de communication, d'Internet, des appareils, etc.?
- La politique de l'organisation explique-t-elle ce qui sera une utilisation acceptable des médias sociaux à des fins commerciales, y compris les publications sur les médias sociaux dans lesquelles l'organisation est identifiée?
- L'organisation a-t-elle une politique qui traite de l'utilisation d'appareils appartenant à des employés dans les activités de l'entreprise?
- L'organisation a-t-elle une politique qui aborde le travail des employés à domicile/ de leurs bureaux à domicile, ainsi que l'utilisation d'appareils mobiles et de systèmes de stockage de données portables (comme les clés USB, les disques durs portatifs, etc.)?

Éducation et formation des employés

- L'organisation a-t-elle des politiques écrites officielles et les employés reçoivent-ils une formation régulièrement, dont l'achèvement avec succès est documenté?
- La formation est-elle donnée pendant l'intégration, lorsque le rôle de l'employé change, de façon continue et lorsqu'il y a un changement important à une politique?
- La formation est-elle documentée et les employés y adhèrent-ils chaque fois qu'ils la terminent avec succès?
- Les employés qui quittent leur emploi reçoivent-ils une entrevue de départ pour leur rappeler leurs obligations continues et pour s'assurer que les actifs informatiques et les appareils sont retournés?

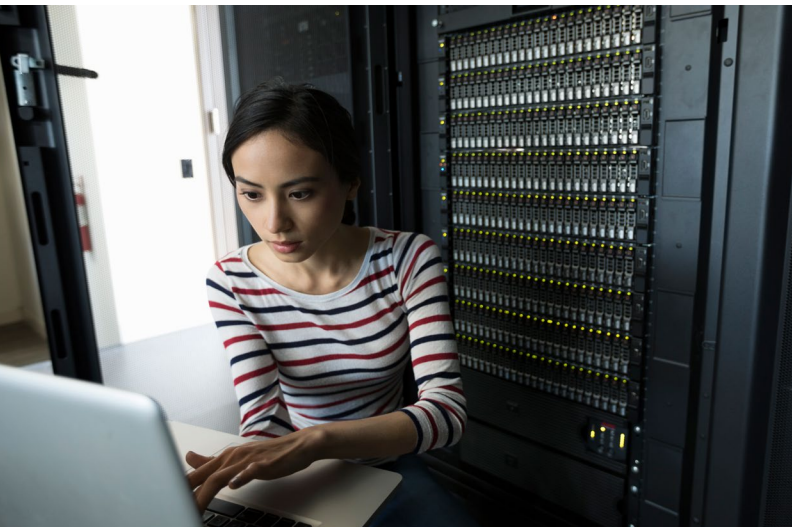


Vérification diligente auprès des fournisseurs

- L'organisation a-t-elle une politique qui établit ce qui constitue une vérification diligente usuelle et suffisante pour tous les fournisseurs qui auront accès, de quelque façon que ce soit, au système de TI de l'organisation?
- Dans le cas des fournisseurs qui fournissent des actifs ou des services de TI, la vérification diligente sera importante lors de la négociation et de l'application des modalités de cybersécurité dans leur contrat, ce dont il sera discuté plus en détail dans la barre latérale Exemples de demandes de renseignements sur le contrôle diligent des fournisseurs.

Exemples de demandes de renseignements sur le contrôle diligent des fournisseurs

- Quel est l'état du cadre de sécurité du fournisseur? Quelles politiques et procédures a-t-il mises en place pour maintenir l'intégrité du cadre ?
- Le fournisseur permettra-t-il d'effectuer des essais de pénétration et d'explorer d'autres vulnérabilités?
- Les installations du fournisseur font-elles l'objet d'une vérification des contrôles internes reconnus par l'industrie? Le fournisseur effectue-t-il des vérifications internes et est-il disposé à faire part des résultats au client?
- Où sont les centres de prestation des services du fournisseur? Où traite-t-il et stocke-t-il les données?
- Quelle assurance contre le risque de cybersécurité le fournisseur détient-il et a-t-il présenté des réclamations au cours des cinq dernières années?
- Le fournisseur fonctionne-t-il conformément aux normes de sécurité reconnues par l'industrie (y compris celles liées à l'infonuagique, le cas échéant)?



Ententes d'accès et de services de TI avec des tiers

La forme la plus élémentaire de contrôle d'accès sont les privilèges d'utilisateur, qui font référence aux droits d'accès des utilisateurs aux systèmes et aux données de l'entreprise. Le principe qui prévaut est celui des « moindres privilèges», qui exige que les utilisateurs ne se voient accorder que le niveau d'accès nécessaire à leur travail.

Le principe des « moindres privilèges » s'applique non seulement aux employés, mais aussi aux fournisseurs et autres tiers. Dans de nombreux cas, ces types de relations seront régis par des contrats, qui peuvent également devenir un élément clé de la préparation à la cybersécurité, avec des dispositions axées sur la prévention, l'intervention, l'atténuation et les mesures correctives.

Il existe deux scénarios généraux avec des tiers : le premier est lorsqu'une organisation conclut un contrat avec un fournisseur réellement pour des services informatiques, et le second est lorsqu'une organisation conclut un contrat avec un fournisseur pour un autre produit ou service qui requiert l'accès au système des TI (par exemple, un fournisseur de services d'éclairage qui a besoin d'accéder aux systèmes des TI d'une organisation pour la surveillance environnementale). Bien que les deux scénarios exigent un contrôle diligent en matière de cybersécurité, les considérations relatives au contrôle diligent sont beaucoup plus complexes dans le premier scénario.

Dans le cas d'une entente de services de TI, le point de départ sera de comprendre les risques de cybersécurité de l'organisation (voir la barre latérale Exemples de facteurs dans l'évaluation du profil de risque de cybersécurité d'une organisation).

De plus, il est essentiel de mener un contrôle diligent à l'égard d'un fournisseur potentiel pour mettre en place le meilleur contrat possible. La structure et les composantes de la solution du fournisseur, ainsi que les capacités et les certifications du fournisseur, les pratiques de gestion des risques et les moyens financiers sont tous des éléments à explorer.

Après avoir établi le profil de risque de cybersécurité de l'organisation et effectué un contrôle diligent approfondi du fournisseur, l'équipe juridique sera alors en mesure de personnaliser les diverses dispositions de l'entente sur les services de TI proposée ayant trait à la prévention des incidents de données, d'intervention, d'atténuation et de réparation.

Parmi les dispositions les plus importantes de l'entente sont celles concernant la répartition des risques. L'interaction entre les déclarations, les garanties, les indemnités et la responsabilité est généralement fortement contestée dans le domaine de la cybersécurité, alors que la jurisprudence continue d'évoluer. Une organisation peut vouloir consulter un conseiller juridique externe possédant une expertise dans ce domaine pour déterminer comment elle souhaite aborder efficacement ces questions et pour discuter des diverses possibilités qui s'offrent à elle.

Sécurité informatique, logiciels malveillants et surveillance

Les défenses des TI sont essentielles à la gestion du risque d'une organisation. Ces défenses devraient être complètes, à jour et adaptées aux menaces actuelles et anticipées. Il est important qu'une organisation s'abonne à un service complet et légitime d'évaluation des menaces (par exemple, les bulletins de cybersécurité du Centre canadien pour la cybersécurité (CCC) et les documents sur les meilleures pratiques)[17]. Il y a aussi des organisations de l'industrie et du secteur public qui s'occupent de l'échange d'information. Par exemple, en 2019, la Banque du Canada a annoncé un partenariat public-privé avec le Groupe sur la résilience du secteur financier canadien afin de coordonner les interventions en cas d'incidents à l'échelle du secteur et de protéger les infrastructures essentielles[18].

Les logiciels antivirus standards de l'industrie et la protection contre les logiciels malveillants devraient être installés, avec des mises à jour constamment installées et documentées.

Exemples de facteurs dans l'évaluation du profil de risque de cybersécurité d'une organisation

- Est-ce que l'organisation fait partie d'un secteur d'activité régi par un cadre réglementaire qui exige certaines mesures de cyberprotection? Par exemple, si une organisation exerce ses activités dans le secteur des services financiers au Canada, l'entente devra être conforme aux règlements et aux lignes directrices en vigueur et émergents promulgués par le BSIF, l'OCRCVM et les ACVM.
- L'organisation exerce-t-elle des activités dans plusieurs juridictions? Où recueille-t-elle, traite-t-elle et stocke-t-elle les données?
- L'organisation est-elle une société privée ou une société ouverte comptant de nombreux actionnaires et soumise à une surveillance des échanges?
- L'organisation traitera-t-elle des renseignements personnels? Ces renseignements comprennent-ils des renseignements personnels sur la santé? Si c'est le cas, les lois actuelles et en évolution sur la protection de la vie privée rentreront en ligne de compte.
- La solution TI sera-t-elle interentreprises (B2B) ou de l'entreprise aux consommateurs (B2C)?
- La solution de TI impliquera-t-elle des interventions de tiers, comme des fournisseurs d'hébergement ou de méthode de paiement?
- L'organisation stocke-t-elle ses données sur place, dans un centre de données local ou dans le nuage?

Les réseaux de l'organisation devraient être protégés contre les attaques internes et externes, et les réseaux sans fil devraient être sécurisés selon les pratiques courantes de l'industrie. Les pare-feu et la détection des logiciels malveillants devraient être de routine et les tests de pénétration devraient être effectués régulièrement (idéalement par une tierce partie indépendante). Des solutions techniques devraient être en place pour détecter et bloquer les activités ou accès suspects.

Les attaques d'ingénierie sociale devraient également être envisagées. Les organisations devraient former leurs employés sur la façon d'éviter d'être victimes d'attaques par hameçonnage, de jumeaux maléfiques (un point d'accès Wi-Fi non fiable qui semble être un point d'accès légitime offert sur place, mais qui a été configuré pour écouter les communications sans fil, où un agresseur trompe les utilisateurs pour qu'ils connectent un ordinateur ou appareil mobile à un point d'accès contaminé en se faisant passer pour un fournisseur légitime), et des clés USB qui semblent avoir été perdues mais qui sont des appareils infectés de logiciels malveillants délibérément implantés.

Assurance contre les risques liés à la cybersécurité

À mesure que le nombre, la portée et les effets des incidents liés aux données augmentent, les organisations cherchent à transférer le risque qui y est associé. La façon la plus courante de transférer le risque consiste à obtenir des polices d'assurance : si le risque est assurable, le risque est transférable. Par exemple, Marsh Inc., un courtier d'assurance mondial, a estimé que le nombre d'organisations qui ont souscrit à une assurance contre les risques de cybersécurité aux États-Unis est passé de 19% en 2014 à 38% en 2018. Ce nombre ne fera qu'augmenter dans les années à venir, à mesure que la sensibilisation au coût élevé et à la prévalence des cyberattaques augmentera[19].

En général, l'assurance contre le risque de cybersécurité est divisée en une assurance de premier bénéficiaire protégeant le titulaire de la police et en une assurance de tiers pour les réclamations d'un tiers à l'encontre du titulaire de la police.

Les polices d'assurance de premier bénéficiaire peuvent couvrir les coûts et les pertes associés à :

a) l'enquête et le processus associé à la détermination de la portée de l'incident, de l'étendue des dommages et à la prise de mesures pour mettre fin à l'incident;

b) fournir un avis aux personnes dont les renseignements les identifiant ont été compromis ou autrement touchés par un incident. Certaines polices peuvent comprendre une couverture pour les services de surveillance du crédit et l'établissement d'un centre d'appels;

c) les services de relations publiques pour contrer la publicité négative qui peut être associée à une enquête sur les données;

d) répondre aux enquêtes du gouvernement;

e) remplacer le matériel ou les logiciels endommagés;

f) répondre aux parties qui vandalisent les données électroniques de l'entreprise;

g) l'interruption des activités, y compris en ce qui concerne les temps d'arrêt, la perte de données, la récupération des données et les coûts liés aux dommages à la réputation; et

h) des poursuites et de l'extorsion. Un incident peut entraîner des frais juridiques ou inclure des coûts liés à la cyber-extorsion, comme le rançongiciel.

Les polices de tiers peuvent couvrir la responsabilité à l'égard de :

a) l'accès non autorisés aux renseignements identifiant des clients;

b) la transmission d'un virus informatique ou d'un logiciel malveillant à un client ou à un partenaire d'affaires tiers;

c) le défaut d'aviser un tiers de ses droits en vertu des règlements pertinents en cas d'incident de données; et

d) dommages potentiels liés à la publicité, y compris les préjudices causés par l'utilisation de médias électroniques, comme l'utilisation non autorisée ou la contrefaçon de matériel protégé par le droit d'auteur, ainsi que les allégations de calomnie, malice et diffamation.

L'assurance contre les risques liés à la cybersécurité peut également couvrir spécifiquement la gestion de crise liée à un incident lié aux données. Cela peut comprendre toutes dépenses liées à la gestion de l'incident, comme l'enquête, les mesures correctives, les avis requis, la mise en place d'un centre d'appels et la gestion des relations publiques, les vérifications de crédit pour les sujets des données, ainsi que les frais juridiques (y compris les amendes, ou les frais pour intenter ou défendre une poursuite).

Étant donné que toutes les garanties de la police d'assurance dépendent des conditions particulières de la police en cause, les organisations qui cherchent à obtenir une assurance de risque en matière de cybersécurité devraient se poser un certain nombre de questions et faire examiner leurs polices par un conseiller juridique.

Exemples de considérations liées à l'assurance de risque en matière de cybersécurité :

Il n'existe aucune politique standard qu'une organisation peut obtenir en matière d'assurance de risque de cybersécurité. Pour déterminer les types de couverture qu'un fournisseur d'assurance inclura dans une police d'assurance de risques données en matière de cybersécurité, l'assureur tiendra compte notamment des facteurs suivants :

a) des renseignements de base sur l'organisation, y compris son secteur d'activité et la nature de ses activités;

b) les types de données recueillies et traitées par l'organisation et la nature des renseignements sensibles dont l'organisation traite;

c) les relations de l'organisation avec les fournisseurs de services sous-traitants et si les évaluations de la sécurité, de la protection des renseignements personnels et des risques sont effectuées à l'interne ou par des tiers;

d) un registre des antécédents d'incidents de perte et des atteintes à la sécurité passées de l'organisation et de leurs répercussions sur l'organisation;

e) l'infrastructure technologique de l'organisation qui cherche la police d'assurance;

f) les politiques de l'organisation actuellement en place pour sécuriser l'accès des utilisateurs;

g) les politiques actuelles de l'organisation en matière de protection des renseignements personnels et de sécurité du réseau; et

h) les mesures techniques prises par l'organisation pour protéger le système informatique[20].

Lorsqu'une organisation approche un fournisseur potentiel d'assurance liée à la cybersécurité et négocie avec lui, elle devrait explorer les éléments suivants :

a) Quels contrôles de sécurité votre organisation peut-elle mettre en place pour réduire la prime?

b) Votre organisation devra-t-elle procéder à un examen des risques en matière de sécurité?

c) Votre organisation conservera-t-elle le droit de choisir son conseiller juridique en cas de litige lié à l'incident?

d) Quelles sont les attentes envers votre organisation pour réduire ou limiter les risques?

e) Votre organisation obtiendra-t-elle une réduction pour chaque année où elle ne présente pas de réclamation en vertu de la police?

f) Votre organisation pourrait-elle présenter sa réclamation en dehors de la période de couverture si elle n'a été en mesure de détecter une intrusion qu'après que plusieurs mois ou années se soient écoulés?

g) Le cas échéant, qui prend la décision de payer ou non une rançon?

Plan d'intervention en cas d'incident de cybersécurité

Jusqu'à présent, ce guide s'est principalement concentré sur les éléments proactifs d'un cadre de cybersécurité. L'autre aspect important de la préparation à la cybersécurité est le plan d'intervention réactif en cas d'incident de cybersécurité.

Un plan d'intervention efficace en cas d'incident repose en définitive sur le soutien de la haute direction. L'élaboration d'un plan d'intervention efficace en cas d'incident exige que la bonne équipe soit impliquée. Un plan d'intervention en cas d'incident devrait être élaboré à l'échelle de l'entreprise et s'appuyer sur l'expérience du personnel clé des principaux intervenants au sein de l'organisation. Habituellement, cette équipe comprendra les représentants principaux des services juridiques, des relations publiques et du marketing, du service à la clientèle, des ressources humaines, de la sécurité de l'entreprise et de la gestion des risques, ainsi que des TI. Idéalement, elle comprendra également des conseillers externes prévérifiés et présélectionnés.

Les responsabilités de l'équipe et les détails additionnels du plan d'intervention en cas d'incident sont présentés à la section suivante, **partie 4**.

Une fois que le plan d'intervention en cas d'incident est rédigé, il ne doit pas être rangé dans un tiroir. Les organisations devraient former, mettre en pratique et simuler des incidents de données pour développer une réponse de type « mémoire musculaire ». Les entreprises les mieux préparées organisent régulièrement des « exercices militaires » pour mettre leurs plans à l'épreuve, accroître la sensibilisation des gestionnaires et parfaire leurs capacités d'intervention. Les conseillers juridiques externes, qui ont une compréhension approfondie du fait d'avoir géré des dizaines d'incidents liés aux données, seront souvent invités à faire la simulation et à évaluer la réponse de l'organisation.

Il est également important de noter qu'en cas d'attaque par rançongiciel, il pourrait ne pas être possible de récupérer une copie stockée électroniquement du plan d'intervention en cas d'incident. Les organisations devraient être préparées en mettant à la disposition des intervenants clés des copies physiques du plan d'intervention en cas d'incident.

Le plan d'intervention en cas d'incident devrait être complet et traiter de chaque étape de l'incident de cybersécurité. Ses composantes devraient comprendre au minimum :

1. Une équipe de base interne de décideurs, comprenant le leadership de la haute direction, les services juridiques, les relations publiques et le marketing, le service à la clientèle, les ressources humaines, la sécurité de l'entreprise et la gestion des risques, ainsi que les TI.

2. Des ressources externes avec des dispositifs de retenue en place, en particulier en ce qui concerne les conseillers juridiques et les vérificateurs enquêteurs. Un conseiller juridique externe peut donner des conseils sur les obligations en matière de conformité à la réglementation et aider à orienter la réponse en vue de la préparation à un litige potentiel (notamment en ce qui a trait aux mesures à prendre pour maintenir le privilège de la préparation en vue d'un litige). Les vérificateurs enquêteurs aident à déterminer la source et la portée d'un incident, ce qui, à son tour, éclairera les obligations en matière de rapports et d'avis. Lorsque requis, les fournisseurs de services juridiques et de services d'enquêtes externes devraient être approuvés par le fournisseur d'assurance avant l'incident.

3. Une échelle de gradation de la classification des incidents, avec des classifications plus élevées qui déclenchent une réponse plus robuste.

4. Une carte des données qui comprend les renseignements sensibles dont dispose l'organisation et l'endroit où ils sont stockés.

5. Une liste des parties internes et externes qui doivent être informées d'un incident, ce qui inclut :

   a) les tiers qui ont fourni des renseignements confidentiels ou personnels à l'organisation et qui ont le droit, du point de vue légal ou en vertu d'un contrat, d'être informés d'un incident;

   b) les forces de l'ordre;

   c) les commissaires fédéraux ou provinciaux à la protection de la vie privée qui peuvent avoir compétence;

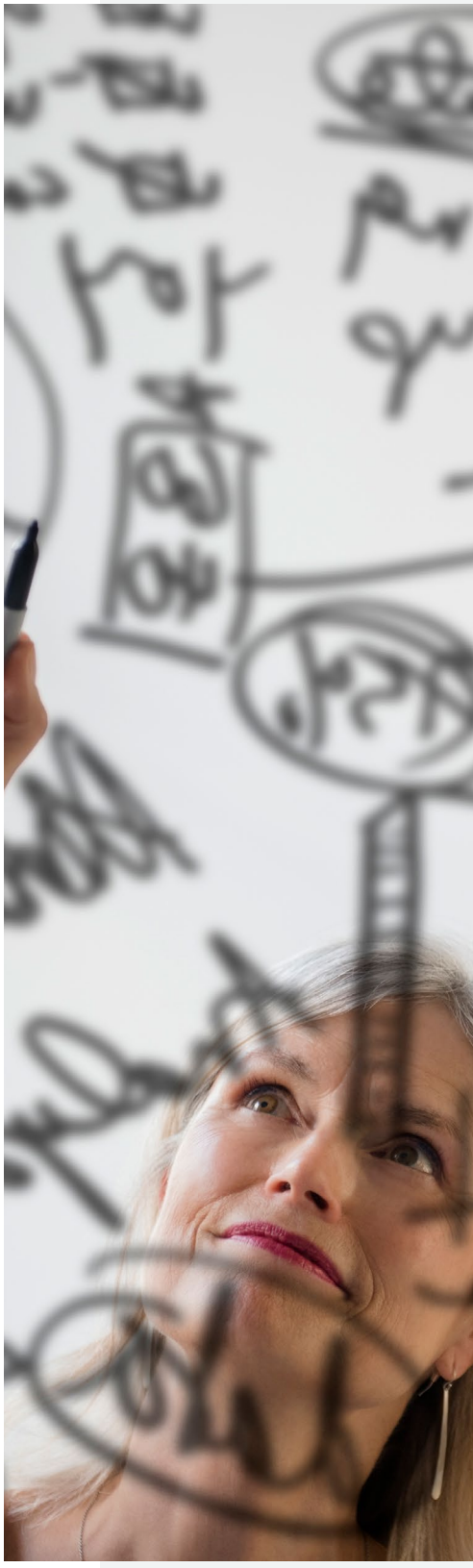
   d) assureur/courtier d'assurance;

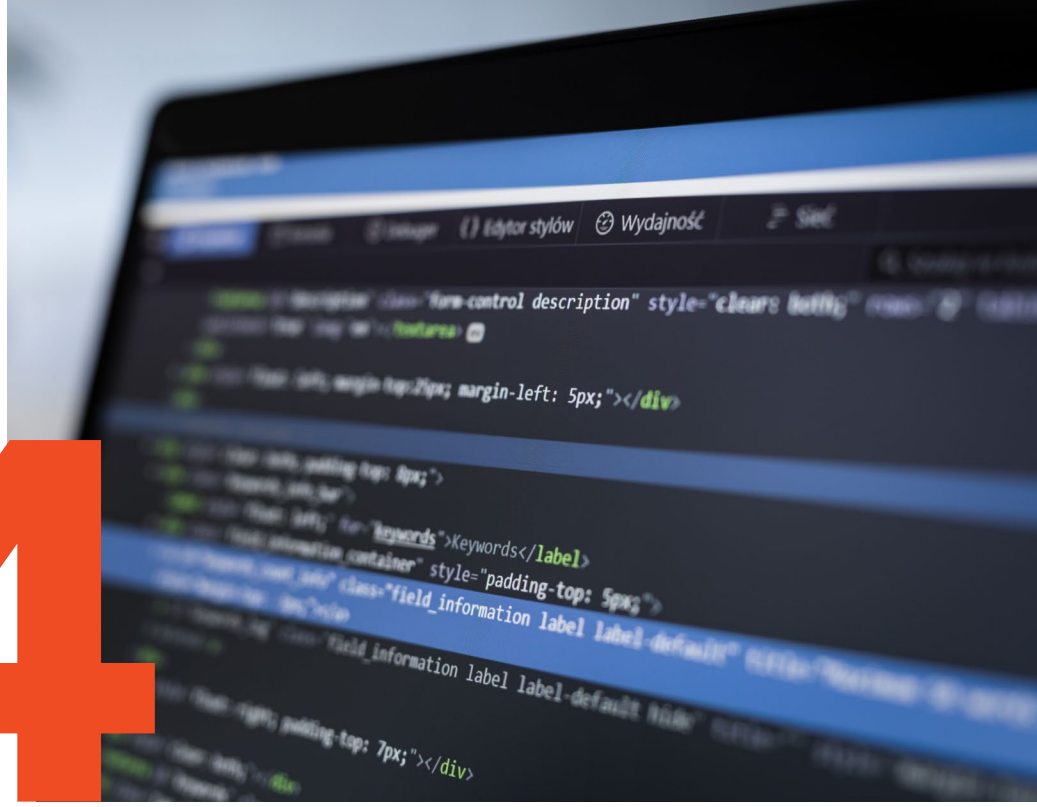
   e) le conseil d'administration; et

   f) des clients et autres personnes et intervenants touchés.

6. Un journal des interventions en cas d'incident.

7. Un aperçu des prochaines étapes et processus pour répertorier les leçons apprises.





04

Que faire lorsque le pire se produit : la mise en oeuvre du plan d'intervention en cas d'incident lié à la cybersécurité

Un plan d'intervention en cas d'incident de cybersécurité devrait être préparé à l'avance, détaillé, testé et bien compris par les membres de l'organisation responsables de sa mise en œuvre. Un plan d'intervention en cas d'incident mettra l'accent sur les efforts d'un groupe diversifié de personnes durant une crise et aidera à prévenir les communications bien intentionnées mais non coordonnées (à l'interne et à l'externe).

Un plan d'intervention en cas d'incident devrait être le fruit de la contribution des intervenants de l'ensemble de l'entreprise. Chaque intervenant devra en fin de compte désigner une personne de son groupe pour diriger l'équipe, ce qui signifie qu'il sera responsable de l'exécution de sa partie du plan et de la production de rapports à la direction.

Plusieurs étapes sont impliquées à tout plan d'intervention en cas d'incident :

Contenir l'incident

Ce ne sont pas tous les incidents liés aux données qui impliquent des pirates informatiques sophistiqués qui compromettent les systèmes des TI d'une organisation. Les incidents physiques (comme les atteintes non électroniques, par exemple des employés qui quittent leur emploi et qui prennent des renseignements avec eux, la perte de documents ou d'appareils, les interruptions de service, le vol d'ordinateurs portables, etc.) sont encore courants. Les organisations devraient noter que le plan d'intervention en cas d'incident ne devrait pas seulement envisager son déploiement en cas d'atteinte électronique, mais aussi dans le cas d'une atteinte non électronique importante.

Selon la portée et la nature de l'incident physique lié aux données, il peut ou non être approprié d'activer le plan d'intervention en cas d'incident et de convoquer l'équipe d'intervention en cas d'incident.

Quoi qu'il en soit, la première étape consistera à enquêter rapidement et à prendre des mesures pour limiter toute perte additionnelle de données. Pour ce faire, on peut limiter l'accès des employés et du public à la zone touchée et changer les serrures et les cartes d'accès, au besoin. Les organisations devraient déterminer s'il est approprié d'aviser les forces de l'ordre. Si une enquête interne ou externe est en train d'être menée, l'organisation devra déterminer quels actifs ont été perdus ou touchés, obtenir des renseignements de suivi (s'il y a lieu), obtenir une surveillance vidéo (si disponible) et, si l'incident est lié à une inconduite de l'employé, tenir compte des répercussions de cette enquête sur les RH.

Si un incident électronique lié aux données s'est produit (par exemple, piratage ou autre atteinte à l'infrastructure de TI ayant entraîné une perte ou une infiltration de données), le confinement sera probablement plus difficile et il est plus probable qu'une organisation devra mettre en œuvre son plan d'intervention en cas d'incident et réunir l'équipe d'intervention en cas d'incident. Ces décisions dépendront en grande partie de l'ampleur de l'incident et du type de renseignements touchés.

Convoquer l'équipe

S'il y a lieu, il faut communiquer avec les différents membres de l'équipe et les mettre au courant. Il pourrait être nécessaire de tenir les communications par téléphone seulement (dans certains cas, par de nouveaux téléphones mobiles) afin d'éviter l'utilisation d'un système de courriel compromis et le risque de fuites. Des communications sécurisées, notamment des téléphones, des ordinateurs portables et des réseaux sécurisés, devraient également être mises à la disposition de la haute direction et d'autres employés essentiels.

Une fois le plan d'intervention en cas d'incident déclenché, des canaux de communication clairs, des structures de signalement et des paliers décisionnels devraient être en place. Lorsqu'il s'agira de décider de ces canaux et structures, il sera essentiel d'avoir déjà envisagé les moyens les plus efficaces d'inclure un conseiller juridique interne et externe afin de préserver le privilège (le cas échéant).

Les membres de l'équipe varieront en réalité selon l'organisation et la nature de l'incident. Toutefois, les responsabilités des membres de l'équipe comprendront généralement les domaines suivants.

Immédiatement après la découverte

Il est essentiel de consigner les renseignements sur une violation, car les récentes modifications apportées à la LPRPDE exigent des organisations qu'elles tiennent et maintiennent à jour des dossiers sur toute atteinte des mesures de sécurité concernant des renseignements personnels sous leur contrôle, sans égard à la gravité de la violation.

La découverte : Consignez la date, l'heure, l'emplacement et la durée de l'atteinte (par exemple, s'agit-il d'une incursion ponctuelle ou si le logiciel malveillant a résidé pendant des mois?). Documentez qui a découvert l'atteinte et comment.

L'atteinte : Consignez les détails de la violation (p. ex, point d'entrée, méthode d'intrusion, systèmes touchés, accès, suppression /modification ou prise de renseignements).

Données : Documentez les détails des données compromises (par exemple, qui sont les personnes touchées? Où se trouvent les personnes touchées? Quel type de renseignements a été compromis? Les renseignements étaient-ils chiffrés? Combien de dossiers sont touchés?).

S'il y a lieu, commencez immédiatement à marquer tous les rapports écrits et autres renseignements générés comme étant « Privilégiés et confidentiels : préparés selon les instructions des avocats en prévision d'un litige ».

Les services juridiques et de la conformité à la réglementation devront :

- En collaboration avec un conseiller juridique externe, mettre en œuvre un protocole sur les privilèges;
- Déterminer si, quand et comment aviser les personnes concernées, les médias, les forces de l'ordre, les organismes de réglementation gouvernementaux et d'autres tiers (tels que les émetteurs de cartes, les banques, etc.);
- Avoir établi des relations avec un conseiller juridique externe avant un incident et gérer un conseiller juridique externe pendant une intervention en cas d'incident;
- Gérer tous les avis prévus par la loi dans toutes les juridictions et la communication avec les commissaires à la protection de la vie privée, les organismes de réglementation, etc.;
- Veiller à ce que les documents et les rapports internes soient produits selon les directives du conseiller juridique externe;
- Émettre et assurer le respect des avis de conservation de la preuve en prévision d'un litige;
- Contrôler l'information et identifier les personnes qui figurent sur la liste des personnes qui doivent être tenues informées; et
- Examiner toutes les communications sortantes, les dépôts, les rapports, etc.

Relations publiques/Marketing devront:

- Connaître les canaux et les intervenants de l'industrie et avoir déterminé les stratégies clés en matière de relations publiques avant qu'un incident ne se produise;
- Avoir un plan de communication interne pour mettre l'accent sur la confidentialité, les mesures appropriées prises par les employés si les médias communiquent avec eux et un plan d'intervention si des renseignements sur l'incident sont divulgués; et
- Suivre et analyser la couverture médiatique et élaborer un plan pour répondre, si nécessaire, à la couverture négative.

Le service à la clientèle devra :

- Répondre aux demandes des clients
- Être en mesure de justifier pourquoi les demandes de renseignements sur les incidents seront traitées à l'interne ou si un centre d'appels sera mis en place; et
- S'il y a lieu, mettre en place un centre d'appels et un programme de protection des consommateurs (voir ci-dessous pour plus de renseignements et la barre latérale du centre d'appels).

Les ressources humaines devront :

- Gérer les employés pendant l'incident, y compris la réaffectation des ressources humaines, au besoin; et
- Traiter les enquêtes, les mesures disciplinaires et la cessation d'emploi si l'incident est attribuable à des actes répréhensibles commis par un employé.

La sécurité de l'entreprise et la gestion des risques devront :

- Communiquer avec les forces de l'ordre (ainsi que leurs services juridiques), y compris la GRC, et peut-être le SCRS, le CST, le FBI et les Services secrets, si l'incident est d'une ampleur suffisante;
- Diffuser à l'équipe toutes directives des forces de l'ordre et en assurer le respect; et
- Gérer les risques d'incident, le confinement des zones touchées et l'accès physique.

Le service TI devra :

- Collaborer avec les services d'enquêtes externes en TI pour identifier et supprimer tout code malveillant ou tout autre artefact d'un incident de données, si la source de l'incident est électronique; et
- Participer à la gestion de la preuve et à la mise en place de mesures de conservation de la preuve ainsi qu'appuyer le travail réalise dans le cadre des litiges

Analyser et documenter l'incident

Une organisation devrait commencer à recueillir des renseignements pertinents au moment même où un incident est identifié. Tous les renseignements relatifs à l'incident de données devraient faire l'objet d'un avis de conservation de la preuve en prévision d'un litige afin qu'ils puissent être conservés, recueillis et analysés sous la direction d'un conseiller juridique (et fournis aux forces de l'ordre au besoin/si approprié). Un examen ultérieur par les avocats déterminera quels renseignements sont réellement pertinents à tout litige et quels renseignements peuvent faire l'objet d'un privilège juridique, mais la première tâche consistera à identifier et à préserver les renseignements qui pourraient être pertinents.

À mesure que la cause de l'incident de données devient évidente et que les personnes touchées sont identifiées, une organisation sera en mesure de prévoir comment les renseignements compromis pourraient être utilisés. S'agissait-il de renseignements financiers personnels non chiffrés qui ont fait l'objet d'un piratage malveillant? Ou était-ce la perte d'une clé USB chiffrée avec des noms et des adresses seulement ?

Les premiers renseignements sont beaucoup plus susceptibles d'être vendus sur les marchés noirs sur Internet et utilisés pour la fraude ou le vol d'identité. Une organisation peut alors commencer à prendre des décisions relatives à l'atténuation du risque, la protection des consommateurs et l'application de la loi.

Lorsqu'un incident lié aux données survient, l'organisation n'aura que peu de temps pour recueillir des éléments de preuve essentiels.

Bien que l'équipe interne des TI agisse comme premier répondant en cas d'incident lié aux données, elle n'a souvent pas reçu de formation sur la récupération des données et l'analyse criminalistique et peut parfois faire plus de mal que de bien en endommageant des données critiques ou en manipulant par inadvertance des preuves importantes. Pour cette raison, un cabinet externe offrant des services d'enquête en TI est probablement l'un des premiers fournisseurs externes retenus qui va opérer après un incident de données, en utilisant des logiciels et des protocoles de criminalistique pour effectuer la collecte et la préservation des données à la suite d'un incident de données.

Lorsque des renseignements personnels sont en jeu, les organisations doivent également créer un registre qui demeure disponible pour inspection par le CPVP. Pour en savoir plus, les organisations doivent consulter le site Web du CPVP, qui contient des conseils utiles pour les entreprises, des mises à jour et une foire aux questions[21].

Compétences d'une firme offrant des services d'enquêtes spécialisées en cybercriminalité

Le bon cabinet d'enquêtes spécialisées en TI devra :

- Être en mesure d'identifier et de neutraliser la menace tout en préservant et en manipulant les éléments de preuve au moyen d'une méthodologie en criminalistique éprouvée et solide, à l'aide d'outils et de processus de récupération des données qui sont appuyés par la jurisprudence et l'expérience antérieure en matière de litiges.
- Être en mesure de naviguer à travers des systèmes d'exploitation et des appareils (pas seulement les ordinateurs, mais aussi les ordinateurs portables, les appareils portatifs, les unités GPS et, dans de nombreux cas, les technologies désuètes qui sont encore utilisées).
- Être en mesure de gérer ces étapes critiques d'une manière qui respecte la sensibilité des employés et la culture du milieu de travail, parce que la firme effectuera des entrevues et aura accès au moins temporairement aux postes de travail et aux appareils des employés (et, dans certains cas, aux appareils personnels).
- Être en mesure de former une équipe ayant une expérience démontrée en soutien à un conseiller juridique interne ou externe dans l'élaboration d'un dossier.
- Avoir des personnes clés qui peuvent témoigner et comparaître comme témoins crédibles devant les tribunaux.
- Avoir une compréhension approfondie des questions de privilège et de conservation de la preuve, être en mesure de gérer ces questions et de comprendre le rôle que l'une ou l'autre de ses enquêtes et rapports peut jouer ultérieurement dans les procédures réglementaires et judiciaires.

> **Les organisations devraient avoir ces relations en place avant un incident** et, idéalement, avoir déjà coordonné toute intervention prévue avec leur choix de conseiller juridique externe afin de permettre un transfert harmonieux de la gestion de cette phase critique pendant une intervention en cas d'incident.

Évaluer et gérer les répercussions juridiques

En même temps que l'information est recueillie et préservée, et que les détails sur la nature et l'étendue de l'incident deviennent de plus en plus clairs, l'organisation devra également tenir compte des risques de litige découlant de l'incident à moyen et à long terme. Cet élément est souvent négligé dans les étapes initiales de la réponse à un incident de données.

Risque de litige - Actions collectives

Les actions collectives en matière de protection des renseignements personnels sont en hausse. Les actions collectives en matière de protection des renseignements personnels sont généralement intentées a) à la suite d'une atteinte à la protection des données, ou b) en raison de la façon dont une entreprise recueille ou utilise des renseignements personnels.

Il est presque certain qu'à la suite d'un incident important lié aux données, même en raison d'une divulgation accidentelle ou non malveillante, une organisation fera face à au moins une action collective. Il est presque certain qu'une action collective sera intentée au nom de tous les clients susceptibles d'être touchés par la fuite de renseignements personnels. Si une organisation est un émetteur public canadien dont le cours de l'action a chuté immédiatement après l'annonce de l'incident, une personne représentant les actionnaires peut intenter une poursuite contre l'organisation en alléguant que la divulgation publique continue de l'organisation au sujet de l'état de ses systèmes de cybersécurité était trompeuse.

Des actions collectives peuvent également être intentées en réaction aux pratiques des entreprises en matière de collecte, d'utilisation et de divulgation de données. Comme les clients et les parties prenantes affirment de plus en plus avoir une attente raisonnable que leurs renseignements seront protégés par les entreprises avec lesquelles ils font affaire, des réclamations ont été déposées alléguant que les entreprises ont (a) enfreint leur politique de protection des renseignements personnels, (b) recueilli, utilisé ou divulgué des renseignements personnels sans obtenir le consentement approprié, ou (c) divulgué des renseignements personnels à des tiers sans obtenir au préalable le consentement approprié[22], Bien que les tribunaux aient souvent refusé d'autoriser de telles demandes, à mesure que la collecte de renseignements personnels augmente, nous pouvons nous attendre à ce que les consommateurs soient plus à l'affût et qu'un plus grand nombre d'actions collectives soient déposées dans ce domaine à l'avenir.

Au Canada, une action collective de consommateurs ou d'actionnaires sera presque toujours intentée devant les tribunaux provinciaux (plutôt que fédéraux). Une seule action collective peut être intentée dans chaque province et les cabinets d'avocats en demande fonctionnent généralement en supposant que s'ils sont les premiers à présenter une demande dans une province donnée, cela décourage les poursuites concurrentes dans la même juridiction. Par conséquent, les cabinets d'avocats en demande intentent généralement une poursuite en réponse à un incident lié aux données dès qu'ils peuvent identifier un demandeur approprié qui pourrait avoir été touché. La demande introductive d'instance ne contiendra probablement que des termes généraux, en insérant simplement le nom de l'organisation et quelques faits de base sur l'incident. Aucune enquête sur le fond d'une affaire ne sera probablement menée avant que l'action collective proposée ne soit déposée (habituellement accompagnée d'un communiqué de presse).

Dans une décision importante rendue par la Cour supérieure du Québec dans l'affaire Equifax[23], le tribunal a décidé que les inconvénients relatifs à l'annulation de cartes de crédit et le stress psychologique causé par le fait de savoir ses renseignements personnels entre les mains de tiers mal intentionnés constituent des contrariétés, craintes et angoisses que toute personne vivant en société doit accepter.

Cette décision constitue un précédent positif pour toute entreprise qui, face à une fraude informatique ou à une cyberattaque, assume ses obligations notamment en avisant les personnes touchées dans la mesure où les dommages pécuniaires ou des troubles et inconvénients significatifs ne sont pas subis par ceux-ci. Ainsi, la simple crainte que les renseignements personnels communiqués soient utilisés et l'angoisse afférente ne suffisent pas nécessairement à entraîner l'autorisation d'une action collective, une condamnation,

même en présence d'une conclusion de faute dans le cadre de la protection des renseignements personnels.

Il faut toutefois nuancer cette affirmation. Cette conclusion n'est pas absolue. La décision de la Cour aurait pu être différente si le demandeur avait eu à assumer des frais pour acheter des services de protection d'identité ou, encore, s'il avait détaillé avec davantage de précisions la nature des dommages psychologiques ou autres qu'il prétendait avoir subis.

Dans le cas d'une action collective intentée devant un tribunal provincial, la disponibilité des causes d'action de de droit commun ou prévues par la loi dépendra de la juridiction.

- Plusieurs provinces ont des causes d'action légales dans les lois sur la protection de la vie privée. Par exemple, la *Privacy Act* de la Colombie-Britannique crée un délit légal d'atteinte intentionnelle à la vie privée si une personne, volontairement et sans droit, viole la vie privée d'une autre personne. Ce délit peut faire l'objet d'une action sans preuve de dommage compensatoire. En raison de ce droit prévu par la loi, il est bien établi en Colombie-Britannique qu'il n'existe pas de délit de *common law* indépendant en matière d'atteinte à la vie privée. Par conséquent, si elles sont soulevées, ces causes d'action de *common law* peuvent être rayées[24].
- Par contre, en Ontario, la Cour d'appel a confirmé dans l'affaire *Jones c. Tsige* qu'il existe un délit d'atteinte à la vie privée en *common law* qui s'applique aux renseignements personnels généraux[25]. Le tribunal a déterminé que la base de cette nouvelle cause d'action était une « intrusion dans la sphère privée » (« intrusion upon seclusion ») fondée sur la question de savoir si la conduite du défendeur était : (1) intentionnelle, (2) une invasion d'affaires privées sans justification légitime, et (3) considérée par une personne raisonnable comme hautement offensive ou comme une cause de détresse. La possibilité qu'une organisation puisse être tenue responsable en vertu de la responsabilité délictuelle d'une « intrusion dans la sphère privée » suite à une atteinte à la protection des données a été plus récemment appuyée par la décision de la Cour supérieure de l'Ontario dans l'affaire *Agnew-Americano c. Equifax Canada*[26]. La jurisprudence relative à l'intrusion dans la sphère privée continue d'évoluer, les avocats de l'action collective plaidant fréquemment ce délit dans des poursuites liées aux données.
- La LPRPDE énonce une cause d'action privée dont peut se prévaloir un plaignant si la plainte donne lieu à un rapport ou est abandonnée par le CPVP. Il n'est pas clair, à l'heure actuelle, si une action collective peut être intentée en vertu de cette cause d'action[27].
- Au Québec, le Projet de loi 64 introduit la possibilité pour une personne d'intenter un recours en dommages-intérêts fondé sur l'atteinte à un droit prévu à la Loi sur la protection des renseignements personnels dans le secteur privé ou à un droit relatif à la protection de la vie privée énoncé dans le Code civil du Québec.
- Parmi les autres actions collectives liées à la protection des renseignements personnels qui ont été intentées en vertu de causes de *common law*, il y a aussi les délits de négligence, le bris de l'obligation fiduciaire, le bris de confiance, le bris des modalités contractuelles régissant la collecte, la conservation et la divulgation des renseignements personnels (y compris lorsqu'il y a un engagement contractuel de se conformer aux lois, ce qui pourrait comprendre les lois sur la protection des renseignements personnels), et le défaut d'avertir les clients après qu'une atteinte à la vie privée est survenue.

> **Il est possible, au Canada, que des actions collectives se chevauchent dans plusieurs provinces; par conséquent, une organisation peut devoir défendre plusieurs cas parallèles en même temps.**

Qu'il s'agisse d'un cas ou de plusieurs, les actions collectives ont tendance à se dérouler lentement (surtout lorsque les faits sont encore découverts et que la loi sur la responsabilité et les dommages-intérêts est, comme ici, incertaine). Il peut s'écouler de trois à cinq ans avant qu'une action collective ne soit jugée ou réglée. C'est pourquoi une organisation devrait inclure, dans l'équipe d'intervention à l'incident, un conseiller externe spécialisé en litige et l'impliquer dès que possible après un incident. Ce sont des conseillers juridiques externes qui portent attention

aux conséquences à long terme (application de privilège, examen des messages publics, etc.), tandis que l'organisation et ses ressources se concentrent sur l'intervention immédiate.

Risque réglementaire

Une organisation peut aussi s'attendre à être au cœur des procédures réglementaires - c'est-à-dire principalement des enquêtes menées par divers commissaires à la protection de la vie privée qui répondent à des plaintes ou agissent de leur propre chef et, selon le secteur d'activités, aussi par les organismes de réglementation des valeurs mobilières, des institutions financières ou de santé publique, et même par les agences des forces de l'ordre.

Les principaux organismes de réglementation dans ce domaine seront les divers commissaires provinciaux à la protection de la vie privée, ainsi que le commissaire fédéral. Une des principales préoccupations d'une organisation qui a subi un incident lié à des données impliquant des renseignements personnels sera de fournir des avis aux divers commissaires à la protection de la vie privée. Voir la **Préparer et envoyer des rapports aux commissaires et des avis aux personnes touchées** ci-dessous pour une discussion sur la présentation de rapports aux commissaires à la protection de la vie privée concernés.

Couverture d'assurance

L'organisation a-t-elle une assurance contre les risques liés à la cybersécurité? Dans l'affirmative, l'incident est-il couvert et dans quelle mesure? Les ententes et les politiques devront être examinées pour répondre à ces questions. De plus, les conventions d'assurance exigent généralement que l'assuré informe rapidement l'assureur d'un incident soupçonné. Dans le contexte du cadre de cybersécurité et du plan d'intervention en cas d'incident d'une organisation, elle doit s'assurer de savoir quand une telle obligation s'applique, de combien de temps elle dispose pour déclarer l'atteinte soupçonnée et quels renseignements elle doit fournir à son assureur.

Une fois que les étapes ci-dessus sont complétées, l'assureur devrait être avisé, mais seulement une fois que le conseiller juridique a été impliqué et qu'il a approuvé la déclaration. Pour en savoir plus sur l'assurance contre les risques liés à la cybersécurité et sur ce qu'elle peut couvrir, voir la **plan de préparation à la cybersécurité et d'intervention en cas d'incident**.

Un assureur peut être en mesure d'imposer son choix de conseiller juridique ou de vérificateur enquêteur en cas d'atteinte. Pour éviter une telle imposition, il est important que l'organisation discute de ces décisions au début d'une relation avec un fournisseur d'assurance donné.

Indemnisation (par des tiers ou des employés et leur responsabilité)

Lorsqu'un tiers (tel qu'un fournisseur de services de TI) est impliqué dans une perte de données, les ententes pertinentes devraient être examinées relativement aux clauses d'indemnisation et à toute exigence en matière de notification ou d'information. Une fois l'évaluation ci-dessus terminée, le tiers fournisseur de services devrait être avisé, s'il y a lieu, mais seulement une fois que le conseiller juridique a participé à l'évaluation et a approuvé la notification.

Les devoirs et responsabilité des employés peuvent également être en cause. Un examen devrait être effectué pour déterminer si les politiques de l'entreprise ont été suivies ou si les lois ont été violées, et des mesures appropriées et adaptées devraient être prises. Si l'organisation a un environnement syndiqué, des considérations liées à la main-d'œuvre peuvent également être en jeu.

Infractions au Code criminel

Vol d'identité et fraude d'identité (art. 402.2 et 403)

L'usurpation d'identité est la possession et le trafic d'information sur l'identité d'une autre personne lorsque les renseignements seront utilisés dans certains crimes de tromperie énumérés (faux, fraude, etc.). La fraude d'identité consiste à se faire passer pour une autre personne pour le profit de l'usurpateur ou au détriment de la victime.

Utilisation non autorisée d'un ordinateur (par. 342.1)

Constitue une infraction l'accès frauduleux à un ordinateur ou à un système de stockage de données appartenant à quelqu'un d'autre pour télécharger de l'information ou intercepter des communications privées (par exemple, un ancien employé mécontent qui pirate le système des TI d'une organisation).

Méfait à l'égard de données informatiques (art. 430(1.1))

Cette infraction criminalise l'utilisation non autorisée de données qui les rendent moins utiles à son propriétaire. Il est à noter que le vol de renseignements confidentiels n'est pas visé par cette infraction et qu'il est difficile de le faire en vertu de toute autre infraction au Code criminel, car la Cour suprême du Canada a jugé que les renseignements confidentiels n'étaient pas " de la propriété ".

Interception illégale de communications privées (art. 184)

Intercepter ou accéder à une communication privée est illégal lorsque les personnes ont une attente raisonnable de protection de la vie privée.

Terrorisme (art. 83.01 à 83.21)

Le piratage à grande échelle, conçu pour mettre en danger la vie et la sécurité du public ou pour perturber un service essentiel à des fins politiques, religieuses ou idéologiques, peut relever de cette disposition. C'est une infraction de participer à cette activité de piratage, de la faciliter ou de donner des instructions à d'autres personnes d'entreprendre cette activité de piratage.

Forces de l'ordre

Les forces de l'ordre peuvent être impliquées. Cette implication peut se faire de deux façons, soit lorsque les forces de l'ordre s'adressent à l'organisation pour demander des renseignements, soit lorsque l'organisation elle-même demande aux forces de l'ordre de s'impliquer.

Les organisations devraient être au courant des restrictions en matière de divulgation. Si elle est approchée par les forces de l'ordre, une organisation devrait savoir que, selon la juridiction, elle peut uniquement avoir le droit de leur divulguer des renseignements sans le consentement de la personne concernée si elle est tenue de le faire en vertu d'un mandat ou d'une citation à comparaître, ou selon d'autres exigences de la loi.

La question de savoir si et quand une organisation peut divulguer des renseignements personnels demandés par les forces de l'ordre, mais non requis par la loi, est un domaine complexe et en constante évolution.

Les forces de l'ordre peuvent également être impliquées parce que l'organisation a conclu qu'elle est victime d'une infraction criminelle (voir les infractions au Code criminel dans la barre latérale).

Une fois que les forces de l'ordre sont impliquées, celles-ci peuvent demander que les notifications d'atteinte et autres divulgations soient retardées afin de préserver l'intégrité de leur enquête, ou elles peuvent autrement interdire la divulgation de certains renseignements. Cela peut entrer en conflit avec les obligations légales ou contractuelles existantes de l'organisation et, par conséquent, un conseiller juridique devrait participer à toutes les discussions avec les forces de l'ordre.

Réponse au consommateur/client

L'un des groupes d'intervenants les plus importants dans un incident de données est la clientèle d'une organisation. Les consommateurs canadiens ont des attentes élevées non seulement qu'ils soient informés rapidement d'un incident lié aux données, mais que les organisations prennent des mesures immédiates et claires pour les protéger (ou qu'elles permettent aux consommateurs de prendre des mesures pour se protéger). De plus, une organisation peut être tenue d'aviser les personnes touchées, comme il est expliqué plus loin à la **Préparer et envoyer des rapports aux commissaires et des avis aux personnes touchées**. L'écart entre ce que font les organisations et ce que les consommateurs attendent d'elles crée un risque.

Entre autres choses, les organisations devraient envisager d'établir un centre d'appels pour répondre aux préoccupations des consommateurs. De plus, les consommateurs s'attendent souvent à ce que les organisations impliquées dans d'importants incidents de données concernant des cartes de paiement ou des renseignements les identifiant offrent une surveillance du crédit et de l'usurpation d'identité.

En plus d'aider à fidéliser les clients et à préserver la valeur de la marque, une réponse solide et bien pensée peut avoir une incidence importante sur les frais et les dommages liés aux actions collectives potentielles [28].

Centres téléphoniques

Dans le cas de la plupart des atteintes à la protection des données de grande envergure, une décision sera prise d'activer un centre d'appels (plutôt que de traiter avec les clients en utilisant des ressources internes de façon *ponctuelle*). Plus tôt un centre d'appels sera opérationnel, plus tôt une organisation pourra commencer à gérer le message, en limitant le risque réputationnel et en tentant de réduire la perspective d'une action collective.

Considérations du centre d'appels

- Le fournisseur de services peut-il s'assurer que l'organisation se verra attribuer un numéro sans frais unique pour ses clients?
- Ce numéro sera-t-il réellement sans frais et fonctionnera-t-il dans toutes les juridictions touchées?
- Le fournisseur de services peut-il offrir ce service en tout temps, 24h par jour?
- Pendant combien de temps l'organisation prévoit-elle que le centre d'appels demeurera actif? Si cela n'est pas connu, la période d'activation peut-elle être indéterminée?

- L'adhésion aux produits de protection est-elle simple et facile à comprendre? Les organisations devront réfléchir à la façon d'évaluer l'admissibilité des appelants à ces produits; dans la plupart des cas, les entreprises voudront avoir un seuil faible (ou nul) pour éviter d'autres insatisfactions de la part des clients.
- Le fournisseur de services a-t-il des exemples de scripts et de foires aux questions qui peuvent être personnalisés par une organisation?
- Le fournisseur de services possède-t-il des compétences à la fois en français et en anglais? En d'autres langues ?
- Tous les documents devraient être examinés par un conseiller juridique afin d'assurer l'uniformité du message et de la langue. À quelle vitesse le conseiller juridique peut-il examiner et approuver ces scripts et ces foires aux questions?
- Existe-t-il un processus simple pour que les clients adhèrent aux produits de protection?
- L'organisation a-t-elle le dernier mot dans tous les scénarios? Ou bien le fournisseur de services insérera-t-il son propre libellé et profitera-t-il de l'occasion pour présenter ses services aux clients?
- Est-il possible, le cas échéant, de se diriger vers spécialiste de la résolution des fraudes?
- Le fournisseur de services peut-il fournir des services de suivi et de signalement? Les organisations auront besoin de ces renseignements pour surveiller l'avancement de leurs efforts de résolution d'incidents liés aux données. Il faudrait tenir compte de facteurs comme le volume d'appels quotidiens, le type d'appels, la vitesse de réponse et autres paramètres.

Produits de protection

Il existe généralement deux principaux types de produits de protection offerts : protection du crédit et protection contre le vol d'identité.

La protection du crédit implique une surveillance du crédit sans frais pour les clients et avertit les clients s'il y a des activités ou quelque chose de nouveau dans le rapport de solvabilité d'un client.

La protection contre le vol d'identité consiste à surveiller le permis de conduire, le numéro d'assurance sociale et autres documents d'identité de base, et l'activité en ligne d'un client afin de voir si des renseignements personnels sont achetés ou vendus en ligne, et à surveiller les dossiers judiciaires et autres signes de fraude d'identité possible.

Ces produits de protection peuvent ne pas être requis dans tous les cas. Une organisation touchée par un incident lié aux données devra examiner attentivement les produits qu'elle proposera et, si elle décide de ne pas offrir certains produits, comprendre que la décision fera l'objet d'un examen approfondi, surtout s'il apparaît ultérieurement qu'une telle protection aurait pu être justifiée. La prestation de tels services contribue également à atténuer les dommages éventuels, ce qui sera un facteur dans tout litige ultérieur.

Il peut y avoir des différences importantes dans les produits de protection offerts au Canada et dans d'autres pays, comme les États-Unis.

Lorsqu'un incident lié aux données touche les deux juridictions, les entreprises devraient s'attendre à recevoir des plaintes ou des demandes de renseignements sur les raisons pour lesquelles des services meilleurs, plus longs et plus complets sont offerts dans un territoire plutôt qu'un autre. Ces demandes peuvent être réduites si les déclarations publiques de l'organisation mentionnent seulement le fait que ces produits sont mis à disposition, mais ne précisent pas la nature des produits fournis dans chaque juridiction.

Compensation

Dans certains cas, la protection contre la fraude ou la surveillance de l'usurpation d'identité peuvent ne pas être appropriées ou réalisables. Dans d'autres cas, la bonne volonté des consommateurs peut être en jeu. Dans de telles circonstances, une organisation peut vouloir envisager une indemnisation. Idéalement, cette question aura été étudiée bien avant tout incident lié aux données, et une organisation aura une compréhension claire de la forme de cette compensation, de sa distribution, du montant approprié, etc. (comme des cartes-cadeaux à tous les consommateurs qui présentent une preuve d'achat entre les dates d'admissibilité). Les considérations relatives à la compensation devraient être consignées dans le plan d'intervention de l'organisation en cas d'incident.

Préparer et envoyer des rapports aux commissaires et des avis aux personnes touchées

Avis au(x) commissaire(s) à la protection de la vie privée

En pratique, une organisation peut vouloir aviser tous les commissaires à la protection de la vie privée concernés lorsqu'une atteinte survient en utilisant une approche qui assure un processus de notification coordonné qui maintient la cohérence de l'information. Les organisations doivent savoir que, même si les renseignements fournis à un commissaire à la protection de la vie privée sont généralement confidentiels, certains d'entre eux peuvent être divulgués ultérieurement par suite de demandes en vertu des lois sur l'accès à l'information. Il existe maintenant des exigences obligatoires en matière d'avis d'atteinte (à la fois aux personnes concernées et au commissaire à la protection de la vie privée concerné) en vertu de plusieurs lois sur la protection de la vie privée au Canada, notamment la LPRPDE, la Loi sur la protection des renseignements personnels de l'Alberta, ainsi que la législation récemment proposée au Québec (projet de loi 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, dont l'étape de première lecture a eu lieu le 12 juin 2020).

Les organisations sont tenues d'aviser à la fois les personnes concernées et le CPVP à la suite d'une atteinte à la protection des données lorsque certaines conditions sont remplies. Parmi ces conditions, l'organisation doit signaler par écrit au CPVP toute « **atteinte aux mesures de sécurité** » impliquant des renseignements personnels sous son contrôle s'il est raisonnable dans les circonstances de croire que l'atteinte crée un « **risque réel de préjudice grave** » à une personne (ou un « **RRPG** »). Une atteinte aux mesures de sécurité est définie de façon générale dans la LPRPDE comme suit : « Communication non autorisée ou perte de renseignements personnels, ou accès non autorisé à ceux-ci, par suite d'une atteinte aux mesures de sécurité d'une organisation » ou « du fait que ces mesures n'ont pas été mises en place » [29].

La LPRPDE définit un RRPG de façon exhaustive et comprend, entre autres, « la lésion corporelle, l'humiliation, le dommage à la réputation ou aux relations, la perte financière, le vol d'identité, l'effet négatif sur le dossier de crédit, le dommage aux biens ou leur perte, et la perte de possibilités d'emploi ou d'occasions d'affaires ou d'activités professionnelles ». Cette définition étendue du préjudice impose plusieurs nouvelles contraintes juridiques aux organisations.

Le signalement de la violation doit être fait « le plus tôt possible après que l'organisation a conclu qu'il y a eu atteinte ».

De plus, une organisation qui rencontre une violation aura des obligations de déclaration supplémentaires envers d'autres organisations et institutions gouvernementales si elle croit que les autres organisations pourraient être en mesure de réduire leur risque de préjudice.

Formulaire de rapport au commissaire d'atteinte à la LPRPDE

Les organisations qui ont remarqué une infraction qui crée un risque réel de préjudice grave (RRPG) doivent faire rapport au CPVP.

Le formulaire de rapport doit comprendre :

a) Les coordonnées d'une personne ressource au sein de l'organisation.

b) Une approximation du nombre de personnes touchées.

c) Le moment de l'atteinte et ses circonstances.

d) Une description des mesures de sécurité en place au moment de l'atteinte et des renseignements personnels en cause.

e) Les mesures prises pour aviser les personnes touchées et stratégie d'atténuation.

Ces vastes exigences obligatoires en cas de violation forcent une organisation à faire appel à un conseiller juridique externe dès qu'une violation est détectée afin de satisfaire à l'exigence de la déclaration « le plus tôt possible » prévue à la LPRDE. La non-conformité peut entraîner des sanctions sévères dont il est question ci-dessous.

Pénalités : Une organisation peut être passible d'amendes pouvant atteindre 100 000 $ CA par infraction pour avoir sciemment enfreint les exigences en matière de notification. Au début de 2019, Innovation, Sciences et Développement économique Canada a fait remarquer que « la menace de sanctions financières incite les organisations à prêter attention » et a invité le Parlement à aller au-delà des dispositions actuelles de la LPRPDE et à « renforcer le cadre de protection des renseignements personnels du Canada ». Il demeure fort possible que les modifications législatives subséquentes se traduisent par une application plus stricte et des amendes plus lourdes.

Confidentialité : La LPRPDE donne au Commissaire le droit de rendre public tout renseignement qui est porté à son attention dans l'exercice de ses fonctions, ainsi que tout renseignement figurant dans les rapports d'avis d'atteinte à la sécurité au CPVP, s'il estime que cela est dans l'intérêt public[30]. Cela va au-delà du pouvoir de « de nommer et de blâmer » les contrevenants que le CPVP avait déjà en vertu du régime antérieur de la LPRPDE.

Ensemble, ces dispositions imposent aux organisations des obligations plus strictes en matière de protection des renseignements personnels, de consentement et de notification des violations. Les organisations doivent continuer d'équilibrer ces nouvelles obligations avec la nécessité de réduire au minimum les coûts financiers et réputationnels découlant d'une atteinte à la protection et à la sécurité de données. Les changements apportés par la *Loi sur la protection des renseignements personnels numériques* ont compliqué l'atteinte de l'équilibre recherché, rendu la non-conformité plus coûteuse et rendu encore plus nécessaire un plan d'intervention bien pensé en cas d'incident.

Les plaintes déposées par des particuliers auprès d'un commissaire à la protection de la vie privée donneront lieu à des enquêtes discrètes visant à résoudre le problème en cause, mais les commissaires à la protection de la vie privée peuvent aussi ouvrir une enquête de leur propre chef sur toute question relevant de leur compétence. De telles enquêtes sont plus probables lorsqu'il y a de multiples plaintes individuelles, lorsque la portée de l'incident de données est importante ou concerne des renseignements

particulièrement sensibles, lorsqu'il y a un problème de politique publique plus important ou qu'il faut obtenir des conseils (comme un nouveau type de service ou un nouveau modèle d'affaires), ou lorsque le commissaire à la protection de la vie privée estime que les intérêts des consommateurs ou du public n'ont pas été adéquatement protégés par la réponse de l'organisation.

Avis aux personnes touchées

Lorsqu'il existe un risque réel de préjudice important, l'organisation doit également aviser les personnes concernées. L'avis doit être " donné dès que possible après que l'organisation ait déterminé que l'infraction a été commise. "

L'avis doit être **visible** et contenir suffisamment de renseignements pour aider les personnes touchées à atténuer le risque de préjudice. Les avis envoyés aux personnes touchées doivent satisfaire aux exigences de forme et de contenu énoncées à l'article 10.1 de la LPRPDE, ainsi qu'au *Règlement sur les atteintes aux mesures de sécurité*. Plus précisément, les organisations doivent aviser les personnes de toute atteinte à la sécurité de leurs renseignements personnels qui constitue un RRPG dès que possible. Un avis doit contenir suffisamment de renseignements pour s'assurer que la personne comprend les risques posés par l'atteinte et les mesures qu'elle peut prendre, le cas échéant, pour réduire ou atténuer le préjudice. Cette notification doit comprendre :

- une description des circonstances de la violation;
- la date à laquelle ou la période durant laquelle la violation a eu lieu (ou, si elle est inconnue, la période approximative);
- une description des renseignements personnels qui font l'objet de l'atteinte (dans la mesure où ils sont connus);
- une description des mesures que l'organisation a prises pour réduire le risque de préjudice pouvant résulter de l'atteinte;
- une description des mesures que les personnes touchées pourraient prendre pour réduire le risque de préjudice qui pourrait résulter de l'atteinte ou pour atténuer ce préjudice; et
- les coordonnées permettant à la personne concernée de se renseigner davantage au sujet de l'atteinte.

S'assurer qu'une personne reçoive un avis compréhensible lui permettra d'identifier les risques et de prendre des mesures pour se protéger de ces risques, au besoin. Lorsqu'il n'est pas possible d'aviser directement les personnes concernées, il peut être nécessaire d'envoyer un avis indirect (par l'entremise d'annonces dans les journaux, en ligne ou d'autres avis).

Obligations de tenue de registres

En vertu de la LPRPDE, les organisations sont tenues de « " tenir un registre de toute atteinte aux mesures de sécurité concernant des renseignements personnels sous leur contrôle », peu importe l'étendue de l'atteinte ou la sensibilité des renseignements personnels en cause[31]. Une atteinte « aux mesures de sécurité » désigne toute perte « de renseignements personnels, tout accès non autorisé à ces renseignements ou toute communication non autorisée de ces renseignements » à la suite d'une atteinte aux mesures de sécurité ou du fait que ces mesures n'ont pas été mises en place[32]. L'obligation de conservation d'un registre de toutes les atteintes à la sécurité des renseignements est déclenchée par toute atteinte,

même si l'organisation détermine qu'il n'y a pas de RRPG en découlant. Toutefois, un **RRPG** déclenche l'obligation de le signaler au CPVP et d'aviser les personnes touchées et, possiblement, certains tiers.

Les organisations doivent également « donner au commissaire l'accès au registre » sur demande, ou en fournir une copie[33]. La période de conservation du registre est de deux ans et le registre doit contenir tout renseignement permettant au commissaire de vérifier la conformité aux dispositions obligatoires de la LPRPDE en matière de notification des atteintes à la sécurité des données[34]. Le fait de contrevenir sciemment aux dispositions relatives à la notification obligatoire est une infraction qui entraîne une pénalité pouvant aller jusqu'à 100 000 $. L'exigence de tenue d'un registre est particulièrement importante, car le CPVP a indiqué qu'il effectuera des inspections sectorielles des registres des atteintes à la sécurité des données.

Comment préparer les inspections des dossiers de violation

Pour nous préparer aux inspections des registres des atteintes à la sécurité des données, nous recommandons aux organisations de prendre les mesures suivantes

1. Assurez-vous que votre organisation tient un registre de chaque atteinte réelle ou potentielle aux mesures de garanties de sécurité, notamment :

- **a)** les dossiers qui contiennent tout ce que vous devez inclure dans un rapport au commissaire si votre organisation a signalé la violation (conformément au **Règlement sur les atteintes aux mesures de sécurité**); et
- **a)** Votre cadre d'évaluation pour déterminer si une atteinte aux mesure de sécurité entraîne un risque réel de préjudice important pour la personne touchée, y compris le fondement de votre décision à l'effet qu'il n'était pas nécessaire de signaler l'atteinte (c'est-à-dire sur quelle base vous avez conclu que, dans les circonstances, vous ne croyiez pas que la violation créait un risque réel de préjudice important pour la personne touchée).

2. Vérifiez vos registres pour vous assurer qu'ils comprennent tous les renseignements exigés par le **Règlement sur les atteintes aux mesures de sécurité.**

3. Songez au nombre d'atteintes potentielles aux mesures de sécurité qui ont fait l'objet d'une enquête de la part de vos services de protection des renseignements personnels, juridiques et de conformité. Si le nombre est faible ou nul, interrogez-vous sur la possibilité que des atteintes aient eu lieu sans qu'elles ne soient signalées. Des atteintes fréquentes incluent les appareils perdus ou volés (téléphones, ordinateurs portables, disques durs, etc.), les courriels mal acheminés et les tentatives d'hameçonnage. L'un des défis que posent les avis relatifs aux atteintes aux mesures de sécurité est que les employés ne savent pas toujours qu'ils doivent signaler l'atteinte. Un autre défi est que de nombreuses équipes de sécurité traitent les atteintes aux mesure de sécurité simplement comme un problème de sécurité et ne transmettent pas l'information au service juridique ou à d'autres membres d'une équipe multidisciplinaire d'intervention en cas d'incident. Par conséquent, il est primordial que votre plan d'intervention en cas d'incident comprenne une formation appropriée des employés en matière d'intervention en cas d'incident et des directives claires quant à la notification aux niveaux hiérarchiques supérieurs.

Considérations internationales

Les incidents de données traversent souvent les frontières internationales. Par conséquent, les organisations doivent être au courant des différentes exigences d'un territoire à l'autre. Il est très important que les conseillers juridiques externes participent à l'élaboration d'une réponse intégrée, car la divulgation dans un pays peut avoir des conséquences dans d'autres.

Par exemple, les organisations qui traitent les données à caractère personnel des personnes concernées résidant dans l'Union européenne (« **UE** »), quel que soit l'endroit où elles ont leur siège ou leur emplacement, doivent se conformer au Règlement général sur la protection des données de l'Union européenne (« **RGPD** »). Le RGPD a rendu obligatoires les notifications de violation dans tous les États membres de l'UE où une violation de données est susceptible d'« entraîner un risque pour les droits et libertés des personnes ». En vertu de l'article 33, paragraphe 1, du RGPD, les organisations doivent aviser[35] l'autorité[36] de surveillance dans les 72 heures suivant la prise de connaissance de la violation. Les sous-traitants de données sont également tenus d'aviser le ou les responsables du traitement[37] « sans délai indu » après avoir pris connaissance d'une violation de données. Conformément à l'article 34, paragraphe 1, le ou les responsables du traitement des données doivent communiquer sans délai la violation de données aux personnes concernées lorsque la violation de données à caractère personnel est susceptible d'entraîner un risque élevé pour les droits et libertés des personnes physiques[38]. Le RGPD prévoit de graves répercussions pour les organisations qui ne respectent pas ses exigences, notamment des amendes allant jusqu'à 4 % du chiffre d'affaires annuel mondial ou 20 millions d'euros (selon le montant le plus élevé)[39].

Les États-Unis ont une législation disparate en matière de protection des données qui affecte ce que les organisations doivent faire en cas d'incident de données. En 2018, la *California Consumer Privacy Act* (« **CCPA** ») a été introduite comme l'un des régimes de protection des données les plus stricts aux États-Unis. La CCPA accorde aux résidents de la Californie un éventail de droits en matière de données[40], ainsi qu'un droit d'action privé en matière de cybersécurité et de protection des données dans certaines circonstances[41].

Satisfaire aux exigences particulières du secteur

Certains secteurs d'activité ont des exigences particulières pour la tenue à jour des renseignements personnels et la notification d'une violation de données. Lors de l'élaboration d'un programme de cybersécurité, il est important de déterminer si votre entreprise est touchée par les règlements sur la protection des renseignements personnels propres à l'industrie.

Soins de santé

Les renseignements personnels liés aux soins de santé sont généralement couverts par les lois provinciales. La LPRPDE ne peut s'appliquer que dans certaines situations, par exemple lorsqu'un hôpital exerce une activité commerciale au-delà de ses activités de base.

L'Alberta a des exigences obligatoires en matière de notification des infractions dans sa *Loi sur l'information sur la santé*[42]. De plus, l'Ontario, Terre-Neuve-et-Labrador, le Nouveau-Brunswick et la Nouvelle-Écosse ont une législation sur la protection des renseignements personnels qui a été jugée « sensiblement semblable à la LPRPDE » ce qui est des gardiens de renseignements sur la santé. L'Ontario est régie par la *Loi sur la protection des renseignements personnels sur la santé*, en vertu de laquelle le Commissaire à l'information et à la protection de la vie privée de l'Ontario a publié des lignes directrices propres au secteur de la santé sur la façon de traiter une violation de données[43].

Cartes de paiement

Les incidents de données impliquant des cartes de paiement, la perte ou l'accès non autorisé aux renseignements des titulaires de cartes soulèvent des considérations particulières relativement au réseau complexe des acteurs dans la chaîne de traitement des paiements et les diverses interrelations contractuelles. Bien qu'il n'existe actuellement aucune obligation légale ou réglementaire au Canada d'aviser les fournisseurs de cartes de paiement ou les banques émettrices en cas d'incident de données, de telles obligations pourraient bien découler des diverses relations contractuelles entre (et parmi) l'organisation commerçante et les diverses banques et exploitants de réseaux de cartes de paiement relativement à l'utilisation et à l'émission de cartes de paiement.

Il peut y avoir obligation de se conformer aux normes sectorielles. Le Conseil des normes de sécurité de l'industrie des cartes de paiement a été fondé par des exploitants de réseaux de cartes de paiement de premier plan. Les organisations qui acceptent des opérations par carte de paiement - y compris les acquéreurs, les fournisseurs de services et les commerçants - de l'une ou l'autre de ces marques de paiement doivent se conformer aux exigences de la Norme de sécurité des données de l'industrie des cartes de paiement (« **PCI-DSS** »)[44]. Bien que le Conseil des normes de sécurité ait le pouvoir exclusif d'établir des exigences, il ne participe pas à l'application de la loi. Les exploitants de réseaux de cartes de paiement elles-mêmes sont responsables de la conformité de toutes les opérations effectuées avec leurs propres cartes[45]. Ils y parviennent en appliquant les politiques avec leurs banques membres (acquéreurs). Les banques membres, à leur tour, font respecter la conformité avec les commerçants. Par conséquent, si une organisation souhaite traiter les principales cartes de crédit, elle doit le faire par l'intermédiaire des membres des exploitants des réseaux de cartes de paiement, qui exigent des mesures de conformité PCI-DSS dans leurs contrats de service.

La PCI-DSS exige que la documentation soit élaborée et tenue à jour, que des contrôles de sécurité préventifs et de détection soient mis en place et que des processus soient en place afin de repérer et de contrer les tentatives de violation de

sécurité le plus rapidement possible. Un prestataire de sécurité spécifié PCI-DSS (« **PFI** »), une firme offrant des services d'enquêtes technologiques approuvé comme auditeur de sécurité qualifié par les exploitants de réseaux de cartes, effectuera des examens périodiques de la conformité d'une organisation aux normes PCI-DSS et produira des rapports qui recommanderont ou refuseront le maintien de la certification[46]. Les organisations non conformes sont assujetties à des frais d'opération plus élevés imposés par leurs banques acquéreuses, à des pénalités contractuelles imposées par les exploitants de réseaux de cartes de paiement, à une responsabilité plus élevée en cas d'incident de données et pourraient courir le risque de perdre l'autorisation de traiter les opérations par carte de paiement.

Il peut être nécessaire d'envoyer plusieurs avis sectoriels supplémentaires. Lorsqu'un incident lié aux données survient, l'organisme compromis est souvent tenu (conformément aux règles et aux exigences applicables du secteur des cartes de paiement pour les acquéreurs, les émetteurs et les exploitants de réseaux de cartes de paiement participants) d'aviser les banques acquéreuses et les exploitants de réseaux de paiement participants, et peut être contractuellement tenu de faire appel à un PFI autorisé pour enquêter sur le problème de sécurité, déterminer la cause sous-jacente et faire rapport aux exploitants de réseaux de paiement participants touchées et autres. L'enquête du PFI sera souvent menée en même temps que l'enquête interne du département des services technologiques de l'organisation.

La PCI-DSS ne fournit pas de directives précises sur la façon de gérer une atteinte à la sécurité. Chaque marque de carte de paiement a ses propres politiques et procédures, et celles-ci peuvent différer d'une marque à l'autre. Par exemple, certains exploitants de réseaux de cartes exigent une notification immédiate dès la confirmation d'un incident de données, tandis que d'autres exigent une notification dans les 24 heures suivant la connaissance de cet incident.

Certaines organisations peuvent être tentées de retarder ou d'omettre de rapporter es incidents de données. Toutefois, même si les organisations n'avisent pas la banque et le réseau de exploitants de cartes, il est très probable que ces entités identifieront de façon indépendante l'organisation d'où origine une compromission des données des titulaires de carte. Les banques et les réseaux de cartes de paiement ont mis en place des processus pour identifier la source d'un incident le plus précisément possible.

Un conseiller juridique devrait participer à toutes les discussions avec les enquêteurs PFI et prendre part aux enquêtes connexes. Une organisation peut vouloir consulter un conseiller juridique externe possédant une expertise dans ce domaine pour déterminer comment elle souhaite gérer non seulement l'enquête du PFI, mais aussi ses interactions avec les exploitants de réseaux de cartes, la gestion de sa propre enquête parallèle de son département de services technologiques en matière de cybercriminalité et la préservation des privilèges applicables en contexte d'enquête. Il s'agit d'un domaine complexe aux enjeux élevés, et la gestion stratégique des questions de privilège sera très avantageuse pour l'organisation.

Sociétés ouvertes

La cybersécurité est une préoccupation majeure des organismes de réglementation des valeurs mobilières. En octobre 2018, la Securities and Exchange Commission des États-Unis (« **SEC** ») a publié un rapport d'enquête qui a demandé aux sociétés ouvertes de tenir compte des cyber menaces lorsqu'elles mettent en œuvre des contrôles comptables internes. L'enquête et le rapport qui a suivi ont été motivés par le fait que neuf sociétés publiques avaient récemment été victimes de fraude sous la forme de courriels dans lesquels des criminels prétendaient être des dirigeants d'entreprise ou des vendeurs pour recevoir de grandes sommes d'argent de la part de destinataires sans méfiance. Chaque société a perdu au moins un million de dollars, tandis qu'une autre a perdu plus de 45 millions de dollars. Le président de la SEC Jay Clayton a déclaré : « Les cyber fraudes constituent une menace omniprésente, importante et croissante pour toutes les entreprises, y compris nos sociétés ouvertes. Les investisseurs comptent sur les émetteurs publics pour mettre en place, surveiller et mettre à jour des contrôles comptables internes qui répondent adéquatement à ces menaces[47]. »

Le 1er mars 2019, le New York State Department of Financial Services (« **DFS** ») a mis en vigueur la nouvelle réglementation sur la cybersécurité (le « **Règlement DFS** »). Le Règlement DFS s'applique aux banques, aux compagnies d'assurance et aux autres institutions de services financiers réglementées par le DFS. Le Règlement DFS vise à protéger à la fois les systèmes de technologie de l'information des entités réglementées et les renseignements non publics sur les clients qu'elles détiennent contre la menace croissante de cyberattaque et cyberintrusion. Entre autres, le Règlement DSF exige des mesures dans quatre domaines clés : a) mettre en place un programme de cybersécurité ; b) établir une politique de cybersécurité ; c) désigner un chef de la sécurité de l'information; et d) obligations de signalements et de tenue de registres. Le DFS a également récemment annoncé la création d'une division spécialisée de la cybersécurité spécialisée, qui se concentrera sur la protection des consommateurs et des industries contre les cyber menaces omniprésentes.

> **Les sociétés ouvertes peuvent être tenues de divulguer les risques dans un certain nombre de documents d'information exigés par les lois sur les valeurs mobilières des États-Unis**, malgré l'absence d'obligation explicite de la part de la société ouverte. Une société ouverte doit tenir compte de l'importance de ces risques lorsqu'elle prépare la déclaration exigée en vertu de la *Loi de 1933* sur les valeurs mobilières (« **Securities Act** ») et de *La loi de 1934 sur les échanges de valeurs mobilières* (« **Exchange Act** »). Ces obligations de déclaration peuvent comprendre des obligations de déclarations périodiques, de la Securities Act et de la Exchange Act, des rapports courants et des obligations de divulgation liées aux facteurs de risque.

La SEC a également déclaré que les sociétés ouvertes devraient avoir en place des politiques et des procédures qui aideront à : « (1) se prémunir contre la possibilité que des administrateurs, dirigeants et autres initiés de la société profitent de la période entre la découverte par la société d'un incident de cybersécurité et la divulgation

publique de l'incident afin de spéculer sur la base des renseignements importants non publics sur l'incident, et (2) aider à garantir que la société divulgue en temps opportun tout renseignement important non public s'y rapportant[48]. »

En vertu des lois canadiennes sur les valeurs mobilières, les émetteurs assujettis sont tenus de divulguer les risques dans un certain nombre de documents d'information exigés par les lois sur les valeurs mobilières, y compris dans les prospectus et dans les documents d'information continue, comme les formulaires d'information annuels. Par exemple, les instructions données à la formule 51-102F1 (Rapport de gestion) du Règlement 51-102 (Obligations d'information continue) comprennent une discussion sur les risques qui ont eu une incidence sur les états financiers ou qui sont raisonnablement susceptibles de les affecter à l'avenir, ainsi que sur les risques et les incertitudes qui, selon l'émetteur, auront une incidence importante sur son rendement futur.

L'Avis 11-332 du personnel des ACVM : Cybersécurité pour 2016 (l' « **Avis du personnel de 2016** »)[49], l'Avis 33-321 du personnel des ACVM : Cybersécurité et médias sociaux (l' « **Avis du personnel de 2017** »)[50] et l'Avis multilatéral 51-3477 du personnel des ACVM (l' « **Avis multilatéral** »)fournissent des conseils complémentaires aux émetteurs assujettis, aux inscrits et aux entités réglementées sur la façon de gérer le cyber risque.

Dans l'Avis du personnel de 2016, les ACVM présentent d'abord un résumé de ses initiatives récentes visant à surveiller et à gérer les risques liés à la cybersécurité afin d'améliorer la résilience globale des marchés publics et prend également note des initiatives actuelles visant à améliorer l'échange transfrontalier d'information entre les organismes de réglementation en matière de cybersécurité.

L'avis du personnel de 2016 fournit également des liens et des références à un certain nombre de ressources en cybersécurité particulièrement utiles qui ont été publiées par diverses autorités de réglementation des services financiers et divers organismes d'établissement de normes afin d'améliorer la préparation des intervenants du marché à faire face aux cyber incidents. Ces ressources comprennent :

- Guide des meilleures pratiques en matière de cybersécurité de l'OCRCVM[51] [52]
- Guide de planification de la gestion des cyber incidents de l'OCRCVM[53]
- Bulletin #0690-C de l'Association des courtiers en fonds communs de placement (ACCFM)[54]
- Guide d'autoévaluation du Bureau du surintendant des institutions financières (BSIF) sur la cybersécurité[55].

L'Avis du personnel de 2017 fournit sept domaines d'orientation distincts fondés sur un sondage sur les pratiques de cybersécurité que les ACVM ont mené entre le 11 octobre 2016 et le 4 novembre 2016. Le sondage a permis de recueillir les réponses des sociétés inscrites comme gestionnaires de fonds d'investissement, gestionnaires de portefeuille et courtiers du marché exonéré. L'objectif du sondage était de recueillir des renseignements sur les pratiques des entreprises afin de permettre aux ACVM de fournir des conseils efficaces et utiles sur la meilleure façon de se protéger contre le cyber risque. Les sept domaines d'orientation sont les suivants :

1. Mise en œuvre des politiques et des procédures qui traitent des huit domaines suivants et mise à jour fréquentes de ces politiques et procédures en raison de cyber menaces en constante évolution :
    i. l'utilisation des communications électroniques;
    ii. l'utilisation d'appareils électroniques fournis par une entreprise;
    iii. la perte ou l'élimination d'un dispositif électronique;
    iv. l'utilisation d'appareils électroniques publics ou de connexions Internet publiques pour accéder à distance au réseau et aux données du cabinet;
    v. la détection des activités non autorisées internes ou externes sur le réseau ou les appareils électroniques de la société;
    vi. veiller à ce que les logiciels, y compris les programmes antivirus, soient mis à jour en temps opportun;
    vii. superviser les fournisseurs tiers ou les prestataires de services ayant accès au réseau ou aux données du cabinet; et
    viii. signaler tout incident de cybersécurité au conseil d'administration.
2. Formation adéquate des employés sur les pratiques de cybersécurité de la société et planification de la formation en cybersécurité à une fréquence suffisante pour demeurer à jour;
3. Évaluation des risques liés à la cybersécurité au moins une fois par année;
4. Élaboration d'un plan écrit d'intervention en cas d'incident pour répondre à un incident de cybersécurité et le signaler aux supérieurs hiérarchiques;
5. Contrôle diligent approprié en matière de cybersécurité à l'égard des fournisseurs tiers, des consultants et des autres fournisseurs de services qui ont accès aux systèmes et aux données d'une entreprise. Les accords écrits conclus avec ces parties devraient comprendre des clauses relatives aux cyber menaces;
6. Protection des données. Les entreprises doivent utiliser le chiffrement pour tous les ordinateurs et autres appareils électroniques et exiger des mots de passe forts qui doivent être fréquemment changés pour avoir accès à ces ordinateurs et appareils. Les données devraient être sauvegardées régulièrement et les entreprises devraient tester régulièrement leur processus de sauvegarde ; et
7. Couverture adéquate des polices d'assurance d'une entreprise eu égard aux incidents de cybersécurité.

L'Avis multilatéral qui a été adopté par trois commissions des valeurs mobilières, fournit des directives sur le moment de divulguer un incident de cybersécurité et sur la façon de déterminer l'importance relative qui obligerait un émetteur assujetti à divulguer ces renseignements conformément aux lois sur les valeurs mobilières applicables. L'Avis multilatéral indique aux émetteurs la politique nationale 51-201, la formule 51-102F1 et la formule 51-102F2 du Règlement national 51-102 afin de les aider à déterminer l'importance relative. Il est à noter que l'importance relative dépendra de l'analyse contextuelle de l'incident de cybersécurité et qu'il n'y a pas de critère ou de seuil clair pour qu'un tel incident puisse se produire. Dans tout plan de correction d'une cyberattaque, l'émetteur doit indiquer comment évaluer l'importance relative d'une attaque[56].

La SEC a fourni des lignes directrices similaires concernant la divulgation des risques liés à la cybersécurité. En février 2018, la SEC a publié des lignes directrices pour aider les sociétés ouvertes à préparer des divulgations sur les risques et les incidents liés à la cybersécurité les « **Lignes directrices de la SEC** »)[57]. Les lignes directrices de la SEC n'ont pas proposé de nouvelles règles ou de nouvelles modifications de règles qui imposeraient de nouvelles exigences, mais ont plutôt exprimé les opinions de la SEC dans le cadre de divulgation existant. Ces opinions sont néanmoins importantes, car le personnel de la SEC en tient compte lorsqu'il évalue la pertinence des informations fournies par les sociétés ouvertes.

1 **Exigences en matière de divulgation en matière de cybersécurité.** Compte tenu de la fréquence, de l'ampleur et du coût des incidents liés à la cybersécurité, il est essentiel que les sociétés ouvertes prennent toutes les mesures nécessaires pour informer rapidement les investisseurs des risques et des incidents importants liés à la cybersécurité, y compris ceux qui sont exposés à des risques importants liés à la cybersécurité, mais qui n'ont pas encore été la cible d'une cyberattaque. Les lignes directrices de la SEC fournissent des renseignements aux entreprises sur la façon d'évaluer l'importance relative d'un incident lié aux données, sur l'obligation éventuelle de corriger ou de mettre à jour les divulgations en matière de cybersécurité, et sur la communication de renseignements concernant la surveillance de la cybersécurité par le conseil d'administration.

2 **Seuil de signification.** La SEC considère l'information comme étant significative s'il est fort probable qu'un investisseur raisonnable considérerait ces renseignements comme importants lorsqu'il prend une décision de placement ou si un investisseur raisonnable considérerait qu'ils ont modifié de façon importante l'ensemble des renseignements disponibles. Bien que les exigences en matière de divulgation du Règlement S-K et du Règlement S-X ne traitent pas spécifiquement des risques et des incidents liés à la cybersécurité, les risques ou les incidents liés à la cybersécurité pourraient néanmoins être importants en fonction de leur nature, de leur étendue et de leur ampleur « , en particulier en ce qui concerne les informations compromises ou les activités et la portée des activités de l'entreprise…[et] sur la gamme des dommages que ces incidents pourraient causer. »

3 **Facteurs de risque.** Les Lignes directrices de la SEC signalent plusieurs facteurs de risque de cybersécurité que les entreprises devraient prendre en compte dans leur rapport 20-F, notamment : (i) la probabilité de survenance et l'ampleur potentielle des incidents de cybersécurité; (ii) les facettes des activités et des activités de la société qui entraînent des risques importants en matière de cybersécurité et les coûts et conséquences potentiels de ces risques, y compris les risques propres à l'industrie et les risques liés aux tiers fournisseurs et prestataires de services; iii) le risque de préjudice à la réputation.

4 **Négociation d'initiés et cybersécurité.** Les lignes directrices de la SEC mettent de nouveau l'accent sur la restriction des opérations d'initiés en cas d'un incident de cybersécurité, qui pourrait constituer une information non publique importante. La SEC suggère que, même si une entreprise enquête sur un incident de cybersécurité qui n'a pas encore été divulgué publiquement, il serait prudent pour elle de se demander si elle doit restreindre les opérations de ses initiés. Cette restriction pourrait s'appliquer aux personnes des services de TI et aux firmes offrant des services d'enquêtes numérique qui pourraient trouver des renseignements non publics importants dans la réponse à un incident de cybersécurité.

Le bureau des inspections et des examens de la conformité de la SEC (« **OCIE** ») a publié un rapport sur les observations relatives à la cybersécurité et à la résilience. Dans le rapport, l'OCIE a déclaré que les interventions en cas d'incident de cybersécurité comprennent : i) la détection en temps opportun et la communication adéquate et appropriée d'informations importantes concernant l'incident ; et (ii) évaluer la réponse appropriée et les mesures correctives. L'OCIE a noté que de nombreux organismes ayant un plan d'intervention en cas d'incident comprennent les éléments suivants :

Élaboration d'un plan qui prévoit la notification en temps opportun en cas d'incident, un processus de signalement aux supérieurs hiérarchiques et la communication avec les intervenants clés;

Réponse aux exigences de déclaration applicables, incluant les exigences fédérales et étatiques en matière de déclaration, comme rapporter une activité suspecte pour les institutions financières ou divulguer les risques et dlesincidents importants pour les sociétés ouvertes; et

Affectation du personnel à l'exécution du plan, avec des rôles et des responsabilités spécifique en cas d'incident de cybersécurité[58].

05

Vous aider à vous préparer et à réagir

Les incidents de données survenus chez les grands détaillants, les ministères et les organismes de services financiers devraient servir d'avertissement clair à toutes les entreprises canadiennes qui traitent des renseignements personnels. Les consommateurs s'attendent activement à ce que ces entités prennent des mesures de pointe pour protéger les données personnelles et financières.

De plus en plus, les bonnes pratiques de gestion de l'information vont au-delà des questions de protection des renseignements personnels. Des pirates malveillants (de l'extérieur et de l'intérieur) et des demandes de rançongiciels ont ciblé la propriété intellectuelle, les secrets commerciaux et d'autres renseignements commerciaux essentiels, avec des répercussions notables sur le cours des actions, la durée des mandats des administrateurs et des conseils d'administration et la compétitivité de l'industrie. Les clients ont besoin de l'aide de conseillers juridique qui peuvent concilier la conformité à la loi et l'application des codes de conduite et des politiques de protection des renseignements personnels de l'industrie dans diverses provinces et territoires, tout en ayant une connaissance pratique des conséquences commerciales et technologiques, le tout d'une manière qui aidera le client à préserver les divers privilèges applicables dans le cadre d'une enquête.

La cybersécurité, la protection de l'information et des données commerciales et la gestion stratégique de la production et de la conservation de l'information sont des aspects importants de notre pratique. Nos avocats spécialisés en protection des renseignements personnels et en gestion des données offrent une perspective sur tous les aspects de la gestion, de la conversation et du transfert de l'information. L'atténuation du risque pour les clients est toujours notre priorité absolue et nous avons aidé les clients à gérer l'ensemble du cycle de vie des données, notamment en fournissant des conseils aux entreprises qui cherchent à se préparer à un incident important lié à la sécurité des données et à le prévenir. En cas de crise, nous nous appuyons sur une équipe d'avocats et de spécialistes en litige de premier plan qui ont répondu à certains des incidents les plus médiatisés en Amérique du Nord et qui participent à de nombreuses initiatives clés en matière de cybersécurité (privées et publiques) au Canada.

Contacts principaux

Charles Morgan
Co-Leader, Groupe Cyber/Données
Associé, Québec
cmorgan@mccarthy.ca

Dan Glover
Co-Leader, Groupe Cyber/Données
Associé, Ontario
dglover@mccarthy.ca

Katherine Booth
Gestion de risque et de crise | Litige/Actions collectives
Associée, Colombie-Britannique
kbooth@mccarthy.ca

Jade Buchanan
Gestion de risque et de crise | Respect de la vie privée et de la protection des renseignements personnels
Associé, Colombie-Britannique
jbuchanan@mccarthy.ca

Karine Joizil
Gestion de risque et de crise | Litige/ Actions collectives| Respect de la vie privée et de la protection des renseignements personnels
Associée, Quebec
kjoizil@mccarthy.ca

Julie-Martine Loranger
Litige/Actions collectives
Associée, Quebec
jmloranger@mccarthy.ca

Emmanuelle Poupart
Litige/ Actions collectives | Assurance
Associée, Quebec
epoupart@mccarthy.ca

Isabelle Vendette
Litige/ Actions collectives | Respect de la vie privée et de la protection des renseignements personnels | Gestion de risque et de crise
Associée, Quebec
ivendette@mccarthy.ca

Hovsep Afarian
Assurance
Associé, Ontario
hafarian@mccarthy.ca

Heidi Gordon
Gestion de risque et de crise | Gouvernance d'entreprise & Information de sociétés ouvertes
Associée, Ontario
hgordon@mccarthy.ca

Nikiforos Iatrou
Concurrence
Associé, Ontario
niatrou@mccarthy.ca

Christine Ing
Gestion de risque et de crise | Respect de la vie privée et de la protection des renseignements personnels
Associée, Ontario
christineing@mccarthy.ca

Gillian Kerr
Litige/Actions collectives
Associée, Ontario
gkerr@mccarthy.ca

Dana Peebles
Gestion de risque et de crise | Litige/ Actions collectives
Associé, Ontario
dpeebles@mccarthy.ca

Mike Scherman
Gestion de risque et de crise | Respect de la vie privée et de la protection des renseignements personnels
Sociétaire, Ontario
mscherman@mccarthy.ca

Susan Wortzman
Preuve électronique | Gestion de l'information
Associée, Ontario
swortzman@mt3.ca

Kara Smyth
Gestion de risque et de crise | Litige/ Actions collectives
Associée, Alberta
ksmyth@mccarthy.ca

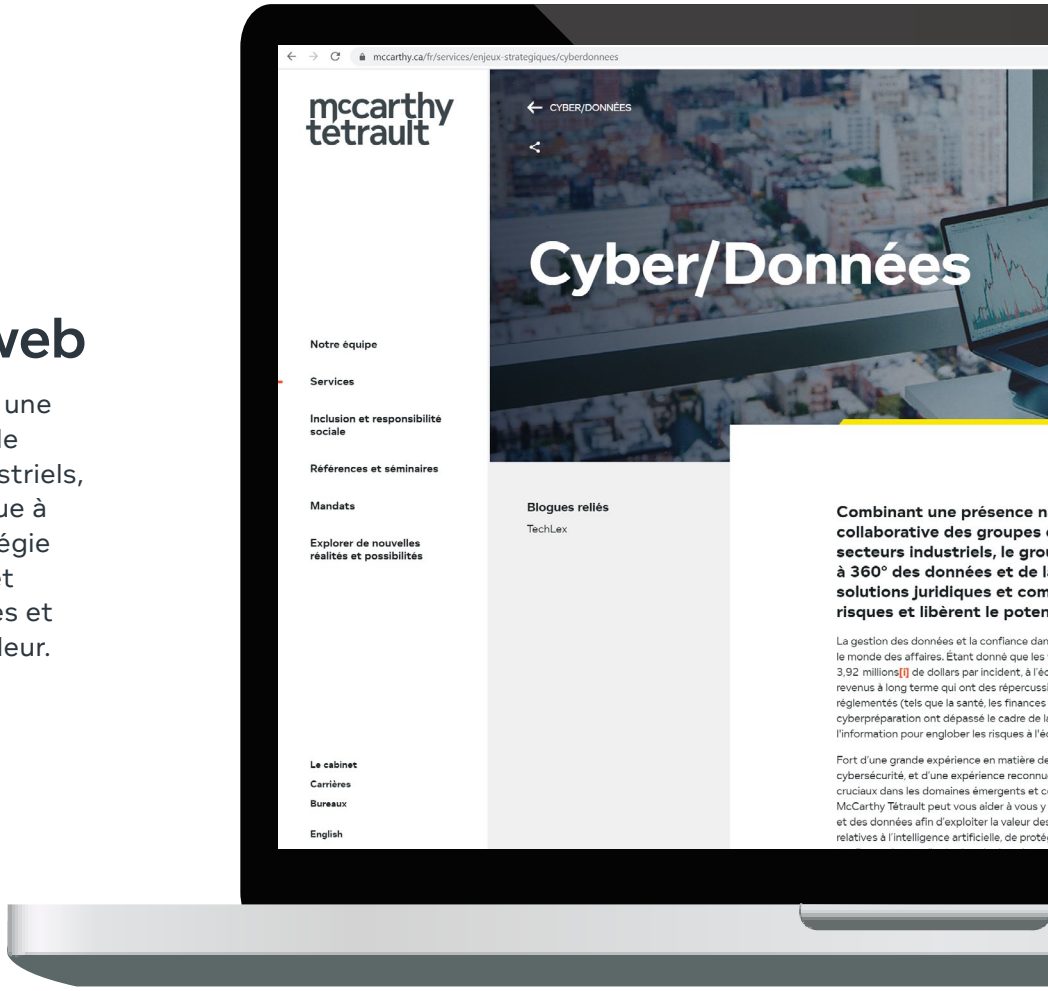
Shana Wolch
Droit du travail et de l'emploi | Litige/ Actions collectives
Associée, Alberta
swolch@mccarthy.ca

Jill Yates
Litige/Actions collectives
Associée, Colombie-Britannique
jyates@mccarthy.ca

Visitez notre site web

Combinant une présence nationale et une approche collaborative des groupes de pratiques dans tous les secteurs industriels, le groupe Cyber/Données offre une vue à 360° des données et de la cyberstratégie pour fournir des solutions juridiques et commerciales qui atténuent les risques et libèrent le potentiel de création de valeur.

www.mccarthy.ca/fr/services/enjeux-strategiques/cyberdonnees



Notes de références :

1 *Lozanski v The Home Depot, Inc.*, 2016 ONSC 5447 (CanLII), **http://canlii.ca/t/gt65j** au paragraphe 70..

2 *Loi sur la protection des renseignements personnels et les documents électroniques,* L.C. 2000, chap. 5, **https://www.canlii.org/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html**.

3 « Le PDG d'Equifax démissionne après le piratage informatique » La Presse, 26 septembre 2017, disponible sur **https://www.lapresse.ca/affaires/economie/services-financiers/201709/26/01-5136765-le-pdg-dequifax-demissionne-apres-le-piratage-informatique.php**.

4 « Two Equifax executives resign in wake of massive data breach », The Hill, 15 septembre 2017, disponible au: **https://thehill.com/policy/cybersecurity/350951-two-equifax-executives-resign-in-wake-of-massive-data-breach** (en anglais seulement).

5 Projet de loi 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, qui a été adopté en première lecture le 12 juin 2020, disponible au: **http://www.assnat.qc.ca/fr/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html**.

6 LPRPDE, *supra*, à l'article 28.

7 Voir, par exemple, « Le commissaire dénonce la lenteur des réformes visant les lois désuètes sur la protection des renseignements personnels », le 27 septembre 2018, disponible au : **https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2018/nr-c_180927/** et « Réforme des lois sur la vie privée : Pour faire respecter les droits et rétablir la confiance envers le gouvernement et l'économie numérique », disponible au : **https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/ar_index/201819/ar_201819/**.

8 « Cybersecurity Is the Key to Unlocking Demand in the Internet of Things », 13 juin 2018, Bain & Company, disponible au: **https://www.bain.com/insights/cybersecurity-is-the-key-to-unlocking-demand-in-the-internet-of-things/** (en anglais seulement).

9 « From Privacy to Profit: Achieving Positive Returns on Privacy Investments, Cisco Data Privacy Benchmark Study 2020 », disponible au: **https://www.cisco.com/c/dam/global/en_uk/products/collateral/security/2020-data-privacy-cybersecurity-series-jan-2020.pdf** (en anglais seulement).

10 Pour plus de détails, voir : Commissariat à l'information et à la protection de la vie privée de l'Alberta, Commissariat à la protection de la vie privée du Canada et Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique, " Obtenir un droit de rendre des comptes grâce à un " de gestion de la vie privée, disponible à l'adresse suivante : **https://www.priv.gc.ca/media/2104/gl_acc_201204_f.pdf**

11 *Signalement des incidents liés à la technologie et à la cybersécurité*, le Bureau du surintendant des institutions financières, janvier 2019, disponible au : **http://www.osfi-bsif.gc.ca/fra/fi-if/rg-ro/gdn-ort/adv-prv/Pages/TCSIR.aspx**.

12 Idem.

13 Bureau du surintendant des institutions financières Canada, « Note d'information : Conseils sur l'auto-évaluation en matière de cybersécurité (octobre 2013), disponible au : **https://www.osfi-bsif.gc.ca/Fra/Docs/cbrsk.pdf**.

14 Autorités canadiennes en valeurs mobilières, « Avis 33-321 du personnel des ACVM : *Cybersécurité et médias sociaux* » (octobre 2017), p. 6, disponible au : **https://www.justice.gov.nt.ca/fr/fichiers/instruments-de-reglementation-des-valeurs-mobilieres/3/33-321/33-321.2017-10-19.fr.pdf**.

15 Idem, p. 13.

16 Tiré de *Dennis Palkon et al. c. Stephen P. Holmes et al.*, No. 2:14-cv-01234 (D.C.N.J., mai 2014), présentation du commissaire de la SEC Luis A. Aguilar du 10 juin 2014, disponible au : **http://www.sec.gov/News/Speech/Detail/Speech/1370542057946** (en anglais seulement) et « Framework for Improving Critical Infrastructure Cybersecurity » (2018) du National Institute of Standards and Technology, disponible au : **https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf** (en anglais seulement).

17 Le matériel du Centre canadien pour la cybernétique est disponible au : **https://cyber.gc.ca/fr/**.

18 « La Banque du Canada annonce la création d'un partenariat visant à renforcer la résilience du secteur financier », juin 2019, Banque du Canada, disponible au : **https://www.banqueducanada.ca/2019/06/banque-du-canada-annonce-creation-partenariat-renforcer-resilience-secteur-financier/?_ga=2.213546960.577339540.1602343071-1302840832.1602343071**.

19 « More Cyber Insurance Buyers as Awareness Grows », mars 2019, Marsh Inc., disponible au : available at **https://www.marsh.com/us/insights/research/cyber-insurance-trends-report-2018.html** (en anglais seulement).

20 Sasha Romanosky et al, « Content analysis of cyber insurance policies: how do carriers price cyber risk? » (2019) 5:1 J Cybersecurity, 8 de 11, disponible au : **https://academic.oup.com/cybersecurity/article/5/1/tyz002/5366419** (en anglais seulement).

21 Commissariat à la protection de la vie privée du Canada, disponible au : **https://priv.gc.ca/fr/**. Voir, en particulier, « Ce que vous devez savoir sur la déclaration obligatoire des atteintes aux mesures de sécurité », octobre 2018, disponible au : **https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/protection-des-renseignements-personnels-pour-les-entreprises/mesures-de-securite-et-atteintes/atteintes-a-la-vie-**

privee/comment-reagir-a-une-atteinte-a-la-vie-privee-dans-votre-entreprise/gd_pb_201810/.

22 Voir par exemple ***Ladas c. Apple Inc.*, 2014 BCSC 1821**; ***Douez c. Facebook, Inc.*, 2014 BCSC 953**, qui est toujours en cours (voir : **2019 (BCSC 715)** (en anglais seulement).

23 *Li c. Equifax, 2019* QCCS 4340

24 ***Ari v. Insurance Corp. of British Columbia*, 2015 BCCA 468**. (en anglais seulement).

25 ***Jones v. Tsige*, 2012 ONCA 32**.

26 ***Agnew-Americano v. Equifax Canada*, 2018 ONSC 275**. (en anglais seulement)

27 ***Haikola v. The Personal Insurance Company*, 2019 ONSC 5982**. (en anglais seulement)

28 Voir, par exemple, ***Lozanski c. The Home Depot, Inc.*, 2016 ONSC 5447** (CanLII) (en anglais seulement), où le juge Perell a fait observer que la réponse à un incident d'un défendeur pourrait bien être un facteur clé qui motive la prise en compte de l'abandon, du désistement ou du règlement d'une action collective : « The case for Home Depot being culpable was speculative at the outset and ultimately the case was proven to be very weak…After the data breach was discovered, there was no cover up, and Home Depot responded as a good corporate citizen to remedy the data breach. There is no reason to think that it needed or was deserving of behaviour modification. Home Depot's voluntarily-offered package of benefits to its customers is superior to the package of benefits achieved in the class actions…By the time the actions against Home Depot came to be settled, there were no demonstrated or demonstrable losses by the Class Members and the Representative Plaintiffs were not even members of the settlement class. Unless one wishes to play pretend, Home Depot was the successful party in resisting a pleaded claim of $500 million », par. 100 à 101 (citation en anglais seulement).

29 Commissariat à la protection de la vie privée du Canada, « Ce que vous devez savoir sur la déclaration obligatoire des atteintes aux mesures de sécurité », octobre 2018, disponible au : **https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/protection-des-renseignements-personnels-pour-les-entreprises/mesures-de-securite-et-atteintes/atteintes-a-la-vie-privee/comment-reagir-a-une-atteinte-a-la-vie-privee-dans-votre-entreprise/gd_pb_201810/**.

30 *LPRPDE, supra,* au paragraphe 20(2).

31 *Ibid.*, section 10.3..

32 *Ibid.*, paragraphe 2(1).

33 *Ibid.*, paragraphe 10.3(2).

34 *Violation du Règlement sur les garanties de sécurité :* DORS/2018-64, section 6.

35 Article 33 du RGPD disponible à : **https://www.privacy-regulation.eu/fr/33.htm#:~:text=Le%20responsable%20du%20traitement%20documente,mesures%20prises%20pour%20y%20rem%C3%A9dier**

36 L'article 4, paragraphe 21, du RGPD définit l'autorité de surveillance " " comme une autorité publique indépendante établie par un État membre conformément à l'article 51, en ligne à l'adresse suivante : **https://www.privacy-regulation.eu/fr/4.htm**.

37 Article 4 (7) du RGPD pour la définition d'un contrôleur " " en vertu du RGPD, disponible à l'adresse suivante : **https://www.privacy-regulation.eu/fr/4.htm**.

38 Article 34 du RGPD pour plus d'informations sur la manière de communiquer aux personnes concernées et lorsque cette communication n'est pas nécessaire, disponible à l'adresse suivante : **https://www.privacy-regulation.eu/fr/34.htm.**

39 Article 83, paragraphe 5, du RGPD pour plus d'informations sur les amendes administratives, disponible à l'adresse **https://www.privacy-regulation.eu/fr/83.htm**.

40 Voir l'article suivant de la Harvard Business Review disponible à l'adresse suivante : **https://hbr.org/2018/07/what-you-need-to-know-about-californias-new-data-privacy-law** (en anglais seulement).

41 Article 1798.150 du Code civil de Californie, introduit par la CCPA.

42 *Loi sur l'information* sur la santé, LSF 2018 c H-5, paragraphe 42(1).

43 Voir Commissaire à l'information et à la protection de la vie privée de l'Ontario, « Signaler une » de violation de la vie privée, disponible à l'adresse **https://www.ipc.on.ca/sante-organismes/le-signalement-dune-atteinte-a-la-vie-privee-au-commissaire/?lang=fr**.

44 Normes de sécurité PCI, mai 2018, disponible à l'adresse suivante : **https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1594333796156** (en anglais seulement).

45 *Ibid*.

46 PCI Security Standards Council, PCI Forensic Investigations, disponible à l'adresse : **https://www.pcisecuritystandards.org/assessors_and_solutions/pci_forensic_investigators** (en anglais seulement).

47 Rapport d'enquête de la SEC « : Les sociétés ouvertes devraient tenir compte des cybermenaces lors de la mise en œuvre des contrôles comptables internes », Securities and Exchange Commission (16 octobre 2018), disponible à l'adresse suivante : **https://www.sec.gov/news/press-release/2018-236** (en anglais seulement).

48 SEC, Déclaration et lignes directrices de la Commission sur les divulgations en matière de cybersécurité des sociétés ouvertes, février 2018, disponible à l'adresse suivante : **https://www.sec.gov/rules/interp/2018/33-10459.pdf** (en anglais seulement).

49 Avis 11-332 du personnel des ACVM : Cybersécurité (27 septembre 2016), disponible à : **https://lautorite.qc.ca/professionnels/reglementation-et-obligations/valeurs-mobilieres/1-procedures-et-sujets-connexes-11-101-a-14-101/avis-des-acvm.**

50 Avis 33-321 du personnel des ACVM : Cybersécurité et médias sociaux (19 octobre 2017), disponible à : **https://lautorite.qc.ca/professionnels/reglementation-et-obligations/valeurs-mobilieres/3-inscriptions-et-sujets-connexes-31-101-a-35-101/avis-des-acvm**.

51 Accessible à **http:// https://www.ocrcvm.ca/industry/Documents/CybersecurityBestPracticesGuide_fr.pdf**.

52 Le 14 novembre 2019, l'Organisme canadien de réglementation du commerce des valeurs mobilières (« **OCRCVM** ») a publié une modification qui est entrée en vigueur immédiatement et qui exige que tous les courtiers en valeurs mobilières assujettis à la réglementation de l'OCRCVM signalent tous les incidents de cybersécurité, accessibles à l'adresse suivante : **https://www.iiroc.ca/documents/2019/d73ffdfa-819e-4560-992b-162d1e2a9c0f_en.pdf** (en anglais seulement).

53 Accessible à **https://www.ocrcvm.ca/industry/Documents/CyberIncidentManagementPlanningGuide_fr.pdf?utm_source=advisor_magazine&utm_medium=link&utm_campaign=exit**.

54 Accessible à **http://mfda.ca/bulletin/Bulletin0690-C/** (en anglais seulement).

55 Accessible à **https://www.osfi-bsif.gc.ca/fra/fi-if/in-ai/pages/cbrsk.aspx**.

56 Avis 51-347 du personnel multilatéral des ACVM : Divulgation des risques et incidents liés à la cybersécurité (19 janvier 2017), disponible à l'adresse suivante : **https://lautorite.qc.ca/professionnels/reglementation-et-obligations/valeurs-mobilieres/5-obligations-permanentes-des-emetteurs-et-des-inities-51-101-a-58-201/avis-des-acvm**.

57 SEC, Déclaration et lignes directrices de la Commission sur les divulgations en matière de cybersécurité des sociétés ouvertes, février 2018, disponible à l'adresse suivante : **https://www.sec.gov/rules/interp/2018/33-10459.pdf** (en anglais seulement).

58 Observations de la SEC sur la cybersécurité et la résilience : Office of Compliance Inspections and Examinations (2019), disponible à l'adresse suivante : **https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf** (en anglais seulement).

mccarthy tétrault

VANCOUVER
Suite 2400, 745 Thurlow Street
Vancouver (Colombie-Britannique) V6E 0C5

CALGARY
Suite 4000, 421 7th Avenue SW
Calgary (Alberta) T2P 4K9

TORONTO
Suite 5300, TD Bank Tower
Box 48, 66 Wellington Street West
Toronto (Ontario) M5K 1E6

MONTRÉAL
Bureau 2500
1000, rue De La Gauchetière Ouest
Montréal (Québec) H3B 0A2

QUÉBEC
500, Grande Allée Est, 9e étage
Québec (Québec) G1R 2J7

NEW YORK
55 West 46th Street, Suite 2804
New York, New York 10036
États-Unis

LONDRES
1 Angel Court, 18th Floor
Londres EC2R 7HJ
Royaume-Uni

www.mccarthy.ca
courriel : info@mccarthy.ca