mccarthy tétrault

Gestion des risques liés à la cybersécurité

Guide pratique pour les entreprises

McCarthy Tétrault LLP
mccarthy.ca

mccarthy tétrault

Gestion des risques liés à la cybersécurité

Guide pratique pour les entreprises

TABLE DES MATIÈRES

PARTIE I: Introduction 3

Prolifération des données 3

Incidents de plus en plus importants et sophistiqués 4

Incidents de plus en plus coûteux 4

PARTIE II: Pourquoi se préparer aux risques 6

Meilleurs résultats 6

Évolution des normes de diligence 6

De la conformité à l'avantage concurrentiel 7

PARTIE III: Votre programme de préparation aux cyberrisques = cadre + plan 8

Cadre de cybersécurité 8

Gouvernance 9

Formation et politiques 11

Accès des tiers et ententes de services TI 13

Sécurité des TI, logiciels malveillants et surveillance 14

Assurance contre les cyberrisques 16

Plan d'intervention 18

PARTIE IV: Exécution efficace du plan d'intervention 19

Contenir les effets de l'incident 19

Réunir l'équipe 20

Analyser l'incident 22

Évaluer et gérer les conséquences juridiques 24

Risque de litige – actions collectives 24

Risque réglementaire 25

Obligations relatives aux cartes de paiement et à la norme PCI DSS 28

Divulgation du risque par les sociétés ouvertes 29
Couverture d'assurance. 31
Indemnisation et responsabilité des tiers ou des employés. 31
Forces de l'ordre 32
Protection des consommateurs/clients 33
Centres d'appel 33
Services de protection 35
Dédommagement. 35

PARTIE I: INTRODUCTION

Qui dit données dit possibilité de perte de données. La façon dont une organisation se prépare à une atteinte à la protection des données – et la gère si elle se produit – a un effet mesurable sur les répercussions d'une telle atteinte. En gérant efficacement un tel incident, qui peut coûter des millions de dollars et ruiner la réputation d'une organisation, on peut le maîtriser et réduire considérablement la gravité de ses conséquences. Par exemple, à la suite d'une atteinte très médiatisée à la protection des données par un logiciel malveillant installé sur les caisses en libre-service de Home Depot, deux sociétés canadiennes ont entamé des actions collectives, réclamant une indemnisation de 500 millions de dollars; les recours ont finalement été réglés pour un montant de 400 000 $. Cette réduction importante est justifiée, dit le juge, au vu de la réponse « exemplaire » de Home Depot[1] :

> Dans l'affaire en question, attendu : a) que Home Depot n'a apparemment commis aucun acte répréhensible; b) qu'elle a réagi rapidement et d'une manière responsable, généreuse et exemplaire aux actes criminels perpétrés contre elle par les pirates informatiques; c) que le comportement de Home Depot n'avait nul besoin d'être géré; d) que la probabilité que les membres du groupe aient gain de cause contre Home Depot tant sur le plan de la responsabilité que de la preuve de dommages consécutifs était négligeable, voire nulle; et e) que le risque d'échec devant les tribunaux et les frais de litige connexes étaient importants et immédiats, j'aurais approuvé l'abandon de l'action collective proposé par M. Lozanski, avec ou sans dépens et sans aucun avantage pour les membres du groupe présumés. [traduction libre]

Prolifération des données

Les renseignements personnels se définissent comme les données pouvant servir à identifier une personne, et leur collecte crée des obligations de protection de la vie privée (expliquant l'existence de lois sur la protection de la vie privée). Avec les progrès technologiques, les organisations recueillent, conservent et transfèrent plus de renseignements personnels sur les consommateurs, les professionnels, les patients et les employés que jamais auparavant. L'accumulation de grandes quantités de renseignements personnels dans d'immenses bases de données augmente le risque d'accès non autorisé à ces informations ainsi que les conséquences qui peuvent en découler. Une seule atteinte à la protection des données personnelles peut aujourd'hui toucher des millions de personnes.

L'adoption croissante d'identifiants biométriques (empreintes digitales ou vocales, reconnaissance faciale, etc.) par les entreprises créent aujourd'hui de nouveaux risques, soit la perte ou la mauvaise utilisation de ces éléments d'identification immuables.

1 *Lozanski v The Home Depot, Inc.,* 2016 ONSC 5447 (CanLII), http://canlii.ca/t/gt65j, parag. 74.

Incidents de plus en plus importants et sophistiqués

Si les incidents connaissent une augmentation croissante, le problème le plus important est leur sophistication grandissante. Les modèles d'affaires des malfaiteurs ont évolué et, en plus de recourir à des méthodes toujours plus complexes, leurs cibles ont changé. Autrefois, le modus operandi consistait à voler des renseignements de cartes de crédit pour effectuer des transactions non autorisées. Aujourd'hui, les cyberadversaires utilisent des méthodes d'ingénierie sociale (comme l'hameçonnage au moyen de courriels frauduleux visant à amener par la tromperie des employés à fournir des informations confidentielles ou sensibles) pour obtenir des renseignements de valeur pour l'entreprise. Ces renseignements sont ensuite monnayés directement par leur utilisation dans le cadre de délits d'initiés, vendus à des concurrents (dans le cas d'une propriété intellectuelle ou d'un secret commercial) ou utilisés pour exiger une rançon.

Les hauts dirigeants d'entreprise craignent de plus en plus les atteintes à la protection des données, et il est désormais communément admis que les sociétés ne doivent pas se demander *si* un tel incident se produira, mais *quand*.

Incidents de plus en plus coûteux

Les atteintes à la protection des données deviennent de plus en plus coûteuses. Si de nouveaux produits (comme les assurances contre les cyberrisques) contribuent à en défrayer les coûts, la réaction la plus fréquente au signalement d'un incident est une poursuite en justice (le plus souvent une action collective). Les dommages-intérêts octroyés ont certes été jusqu'ici relativement minimes, toutefois les coûts de gestion d'une atteinte à la protection des données peuvent être incroyablement élevés.

La réglementation en la matière a un coût. De récentes modifications apportées à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) du Canada ont introduit l'obligation de notification d'une atteinte et une amende de 100 000 $ CA par atteinte en cas de non-respect de cette exigence – s'ajoutant aux frais financiers et aux coûts des atteintes à la réputation qu'engendrent les incidents liés à la confidentialité des données.

AUTRES MÉGA-INCIDENTS RÉCENTS

eBay (2014)	145 millions de personnes touchées
JPMorgan Chase & Co. (2014)	76 millions de ménages et 7 millions de petites entreprises touchés
Home Depot (2014)	56 millions de personnes touchées et 53 millions d'adresses de courriel volées
Yahoo (2014) *incident divulgué en 2016*	500 millions de personnes touchées
Bureau de la gestion du personnel des États-Unis (2014 - 2015)	18 millions de personnes touchées, dont 5,6 millions d'empreintes digitales
Réseau de traitement d'opérations bancaires mondial SWIFT (2016)	Au moins 81 millions de dollars volés
Cabinet d'avocats Mossack Fonseca (2016)	2,6 To de données sensibles sur des politiciens, des criminels, des athlètes professionnels, etc.

Les coûts ne se limitent pas aux dommages : la responsabilité des atteintes à la protection des données peut être imputée au conseil d'administration. Gregg Steinhafel, chef de la direction et président du conseil de Target, a démissionné tout juste après l'incident dont son entreprise a été victime[2]. Un sort similaire a frappé Amy Pascal, qui a quitté ses fonctions de chef de Sony Pictures dans la foulée du piratage de Sony.

COÛTS GLOBAUX DU PIRATAGE DE TARGET EN 2013

Target a enregistré en 2013 et en 2014 des **dépenses de 162 millions de dollars américains** attribuables à l'atteinte à la protection des données, où des pirates se sont introduits dans le réseau de l'entreprise pour accéder aux renseignements sur les cartes de crédit et à d'autres données des clients, qui a touché 70 millions de clients[3]. Target a déclaré que ce montant a été partiellement contrebalancé par des remboursements d'assurance de 46 millions pour 2014 et de 44 millions pour 2013.

De plus, Target a accepté de **régler pour 10 millions de dollars les actions collectives intentées par ses clients**[4]. Les demandeurs doivent faire la preuve des « dommages réels » (y compris, sans s'y limiter, les charges frauduleuses portées aux cartes de crédit), ce qui peut diminuer les coûts, mais cela ne change rien pour Target si les dommages ne sont pas réclamés en totalité. Au bout du compte, le coût du règlement sera probablement supérieur à 10 millions de dollars, car :

- **les avocats des demandeurs ont exigé des dépens de 6,75 millions de dollars;**
- **Target a dû payer les frais de gestion du règlement;**
- **Target a aussi dû adopter des protocoles de cybersécurité et nommer un chef de la sécurité de l'information.**

Enfin, le règlement NE couvre PAS les poursuites intentées contre Target par les émetteurs de cartes de crédit qui ont dû rembourser les frais frauduleux imputés aux consommateurs touchés par le vol de leurs renseignements.

2 « Target CEO resigns after data breach fallout », *CNet online,* 5 mai 2014, en ligne à l'adresse http://www.cnet.com/news/target-ceo-gregg-steinhafel-resigns-after-data-breach-fallout/.

3 « Target Reports Fourth Quarter and Full-Year 2014 Earnings », *Business Wire,* 25 février 2015, en ligne à l'adresse http://www.businesswire.com/news/home/20150225005513/en/Target-Reports-Fourth-Quarter-Full-Year-2014-Earnings#.VQdSZo7F-Sp.

4 « Judge approves Target's $10m hack lawsuit deal », *Toronto Star,* 19 mars 2015, en ligne à l'adresse http://www.thestar.com/business/2015/03/19/target-offers-10m-to-settle-hack-of-40-million-credit-cards.html.

PARTIE II: POURQUOI SE PRÉPARER AUX RISQUES

Meilleurs résultats

Les 72 premières heures sont critiques. Les atteintes à la protection des données ne font pas toutes les manchettes, mais une attaque grave peut bouleverser une organisation durant des mois. Les 72 heures suivant un incident sont particulièrement chaotiques, puisqu'une multitude de problèmes doivent être gérés au moyen d'informations encore incomplètes.

Un plan d'intervention conçu d'avance pour une équipe formée et aguerrie aide grandement à éviter le chaos, car il tient les intervenants clés informés et concentre leurs efforts sur les priorités identifiées. Plus important encore, ce plan aide à organiser les urgences et peut freiner les réactions éparpillées ou le besoin irrépressible de « faire quelque chose ». De plus, une intervention rigoureusement orchestrée réduit les coûts et empêche les fournisseurs externes de prendre trop de place, aider à préserver les preuves permettant d'établir que l'organisation a suivi les normes de diligence applicables et minimise le risque d'atteinte à la réputation.

Évolution des normes de diligence

Un plan conçu, documenté et exécuté avec soin est essentiel pour limiter les pertes de données et les perturbations dans l'organisation. Mais surtout, il contribue à minimiser la responsabilité envers les tiers et les organismes de réglementation, **pourvu** qu'il soit régulièrement mis à jour en fonction de l'évolution des risques et des mesures pour les contrer.

Une organisation pourra, si elle est poursuivie, voir son plan d'intervention (et sa mise en œuvre) évalué par un tribunal pour en déterminer le caractère raisonnable. Avec les nouveaux risques et les nouvelles menaces qui surgissent chaque semaine (et les mesures d'intervention et correctifs correspondants), un plan d'intervention ne saurait être un document statique. Le tribunal chargé d'évaluer le caractère raisonnable d'un plan d'intervention en cas d'incident tiendra compte non seulement des documents préparés par l'organisation, mais aussi du respect des politiques, de l'attribution des ressources techniques, financières et humaines appropriées, ainsi que du degré de participation de la haute direction à la création et à la gestion du plan.

Le caractère raisonnable d'un plan peut être évalué à la lumière des directives réglementaires propres au secteur. Par exemple, le 27 septembre 2016, les Autorités canadiennes en valeurs mobilières (ACVM) ont publié *l'Avis 11-332 du personnel des ACVM – Cybersécurité* (l'« Avis 2016 ») et indiqué que selon elles, il n'est plus suffisant pour les entités réglementées de simplement mettre en œuvre un plan d'intervention réactif en cas d'atteinte à la sécurité. Il faut plutôt, selon les ACVM, un « cadre de cybersécurité » proactif afin de mieux gérer et de réduire les cyberrisques. Les ACVM définissent un cadre de cybersécurité comme « un ensemble de ressources organisationnelles, notamment des politiques, du personnel, des processus, des pratiques et des technologies servant à évaluer et à atténuer les cyberrisques et les cyberattaques » (se reporter à la rubrique « Divulgation du risque par les sociétés ouvertes » ci-après pour une analyse plus détaillée de l'Avis 2016).

De la conformité à l'avantage concurrentiel

Alors que la protection des données était auparavant considérée comme un difficile effort de conformité qui ne rapportait rien, les entreprises avisées réalisent petit à petit qu'une protection améliorée des données et des mesures d'intervention robustes peuvent leur procurer un avantage concurrentiel. Dans une étude réalisée en 2015, 25 pour cent des répondants ont estimé que la haute direction de leur organisation assimile la sécurité à un avantage concurrentiel.[5] Fait encore plus révélateur, **59 pour cent d'entre eux ont affirmé que les cadres supérieurs seront du même avis d'ici 2018.**

5 Ponemon Institute Research Report, *"2015 Global Megatrends in Cybersecurity"*, février 2015. Dans le cadre du sondage, 1 006 chefs de la technologie de l'information et de la sécurité des TI, au fait des stratégies de cybersécurité de leur organisation aux États-Unis, au Royaume-Uni/en Europe et au Moyen-Orient/en Afrique du Nord, ont été interrogés. En ligne à l'adresse http://www.raytheon.com/news/rtnwcm/groups/gallery/documents/content/rtn_233811.pdf.

PARTIE III: VOTRE PROGRAMME DE PRÉPARATION AUX CYBERRISQUES = CADRE + PLAN

Si une atteinte à la protection des données semble presque inévitable, elle peut ne pas être une catastrophe. Les organisations préparées à un tel incident dans le cadre de leur programme de gestion et de prévention des risques liés à la cybersécurité sont beaucoup plus susceptibles de connaître un dénouement favorable en cas d'incident (voire de l'éviter totalement) que celles qui adoptent une approche ponctuelle. Dans le contexte d'atteintes à la protection des données, un « dénouement favorable » se traduit par un processus de résolution d'incident qui attire peu l'attention des médias, réduit les coûts (notamment ceux associés à un possible litige), limite l'atteinte à la réputation, minimise l'intervention des actionnaires et implique un examen limité de la part des organismes de réglementation.

PRINCIPAUX ÉLÉMENTS

1. Gouvernance
2. Formation et politiques
3. Accès des tiers et ententes de services TI
4. Sécurité des TI, logiciels malveillants et surveillance
5. Assurance contre les cyberrisques
6. Plan d'intervention

Un programme de cybersécurité se compose d'un cadre de cybersécurité et d'un plan d'intervention. Un **cadre de cybersécurité** se veut proactif et consiste en un ensemble de ressources organisationnelles, notamment des politiques, du personnel, des processus, des pratiques et des technologies servant à évaluer et à atténuer les cyberrisques et les cyberattaques. Un **plan d'intervention** doit être réactif. Il s'agit d'une initiative prise à l'échelle de l'entreprise, qui établit un protocole pour toute l'organisation, attribue les responsabilités et définit des mesures de suivi des efforts organisationnels déployés pour résoudre les incidents. Il doit comprendre des éléments précis et couvre un vaste éventail de disciplines. Surtout, il doit être exhaustif et détaillé, et ne pas se résumer à de simples cases à cocher ou listes de choses à faire.

Certains éléments clés d'un programme de cybersécurité sont présentés ci-après.

Gouvernance

La cybersécurité ne vise pas qu'à contrer les risques liés aux technologies de l'information. Elle tient également compte des risques à l'échelle de l'entreprise. C'est pourquoi elle devrait faire partie du mandat général de gestion des risques du conseil d'administration.

Le conseil d'administration doit se pencher sur la question de la cybersécurité. En juin 2014, Luis Aguilar, commissaire de la Securities and Exchange Commission (SEC), s'est adressé à la Bourse de New York pour parler des risques liés à la cybersécurité pour le conseil d'administration, précisant que les incidents ont gagné en fréquence et en complexité et qu'ils sont devenus plus coûteux pour les entreprises[6]. Il a mis l'accent sur le rôle des conseils d'administration, soulignant leur responsabilité de s'assurer du caractère adéquat des mesures de cybersécurité de l'entreprise dans le cadre de leur rôle de surveillance des risques.

Les organismes de réglementation commencent à abandonner le principe de la conformité volontaire. Le 13 septembre 2016, le ministère des Services financiers (DFS) de l'État de New York a annoncé un nouveau projet de règlement sur la cybersécurité (le « Règlement ») applicable aux banques, aux compagnies d'assurance et aux autres institutions financières réglementées par le DFS. Le Règlement vise à protéger tant les systèmes d'information des entités réglementées que les renseignements non publics sur les clients qu'ils contiennent contre la menace croissante de cyberattaques et de cyberinfiltrations. Il exige, entre autres, quatre mesures de protection importantes : a) établir un programme de cybersécurité; b) établir une politique de cybersécurité; c) nommer un chef de la sécurité de l'information; et d) répondre aux exigences de signalement et de consignation des incidents.

Au Canada, l'approche a été jusqu'ici quelque peu différente. Si aucune juridiction canadienne n'a encore adopté un règlement semblable, les ACVM ont publié l'Avis 2016 après avoir constaté que de nombreux émetteurs ne communiquaient pas pleinement leur exposition aux cyberrisques. Les ACVM ont également indiqué qu'elles comptent revoir l'information fournie par certains des plus grands émetteurs. (Pour en savoir plus à ce sujet, se reporter à la rubrique « Divulgation du risque par les sociétés ouvertes » ci-après.)

6 « Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus », U .S. Securities Exchange Commission, en ligne à l'adresse <http://www.sec.gov/News/Speech/Detail/Speech/1370542057946>.

Les tribunaux ont également commencé à prendre en compte le rôle des administrateurs dans la gestion des risques liés à la cybersécurité. Le 20 octobre 2014, un tribunal du New Jersey a rejeté une action oblique intentée par des actionnaires de Wyndham Worldwide Corp. (WWC), qui réclamaient des dommages-intérêts, notamment des administrateurs et des dirigeants, au motif de plusieurs atteintes à la protection des données[7]. Cette décision a été la première rendue aux États-Unis dans le cadre d'une telle procédure. Des poursuites similaires ont été intentées dans le district du Minnesota contre les 13 administrateurs et dirigeants de Target. Les demandeurs ont soulevé des allégations de violation de l'obligation fiduciaire et de gaspillage des actifs de la société, entre autres choses. Les actionnaires ont critiqué non seulement la conduite des administrateurs et des dirigeants avant la fuite des données, alléguant que l'incident s'est produit par leur faute, mais aussi leur réaction après la découverte de la fuite, blâmant les administrateurs et dirigeants d'avoir mal agi dans leur manière de communiquer l'incident, de mener l'enquête et de remédier à l'atteinte. Ces plaintes ont également été rejetées[8].

Le jugement contient des exemples de méthodes de surveillance des cyberrisques que les administrateurs et les dirigeants peuvent adopter pour les prémunir de toute responsabilité à l'égard des atteintes à la protection des données.

À la lumière de la décision rendue dans l'affaire Wyndham, nous présentons ici des exemples de mesures que les dirigeants et administrateurs peuvent appliquer pour cerner et évaluer les risques liés à la cybersécurité de leur organisation.

ACTIONS DES DIRIGEANTS ET ADMINISTRATEURS*

POLITIQUES	**Rédiger des politiques de cybersécurité** et adopter des procédures et des contrôles internes, notamment sur le moment et la méthode de divulgation; **Mettre en œuvre des méthodes** de détection des incidents liés à la cybersécurité.
NOMINATIONS	Nommer **un chef de l'information ou un chef de la sécurité de l'information** expérimenté pour rencontrer régulièrement et conseiller le conseil d'administration Songer aussi à **nommer au conseil un expert des questions de cybersécurité** (ou commander une présentation d'expert sur le sujet) et à créer un comité des risques d'entreprise

7 *Palkon ex rel. Wyndham Worldwide Corp. v. Holmes*, No. 2:14-cv-01234 (D.N.J., 20 octobre 2014) [« Wyndham »].

8 *Mary Davis et al. v. Gregg W. Steinhafel et al.*, No. 0:14-cv-00203 (D. Minn., 18 juillet 2014).

EXAMENS ET RAPPORTS	Examiner les **budgets annuels des programmes de protection de la vie privée** et de **sécurité des TI.** Recevoir régulièrement des **rapports sur les atteintes à la protection des données** et les cyberrisques Comprendre clairement **qui, au sein de la direction, est le premier responsable** de la surveillance des risques liés à la cybersécurité et de l'application de pratiques adéquates et efficaces de gestion
ORIENTATION	Déterminer les risques à gérer et à atténuer directement, et ceux qui peuvent être transférés grâce à une **assurance.**

* Tirées de l'affaire Wyndham, de la présentation du commissaire de la SEC Luis A. Aguilar datée du 10 juin 2014 et du document intitulé « Framework for Improving Critical Infrastructure Cybersecurity » du National Institute of Standards and Technology, accesible en ligne à l'adresse <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf>

Formation et politiques

Les politiques et procédures de l'organisation constituent les éléments clés d'un programme de gestion des risques liés à la cybersécurité. Si leur contenu peut varier, les politiques présentent toutefois des éléments communs. Par exemple, quel que soit leur objet précis, sont-elles rédigées en langage clair et compréhensible par les employés de tous les niveaux? Peut-on les consulter facilement (sont-elles affichées sur un intranet, par exemple)? Les employés reçoivent-ils une formation en bonne et due forme?

Le programme de chaque organisation comportera des particularités variables selon la juridiction, le secteur d'activité et la tolérance au risque de l'organisation.

Voici des exemples de particularités que pourraient inclure la formation et les politiques :

SÉCURITÉ DES TI
L'organisation offre-t-elle à l'équipe de sécurité de l'information des outils et de la formation pour l'orienter? Une politique à cet effet peut inclure les éléments suivants :
☐ Contrôle des accès et gestion des mots de passe
☐ Connexions réseau et gestion du pare-feu
☐ Gestion des virus et des maliciels, y compris l'installation des mises à jour et des correctifs, et mécanismes de contrôle des changements
☐ Chiffrement, notamment en transit
☐ Sécurité des réseaux, y compris du réseau sans fil

- ☐ Préparation à l'intervention et à la résolution des incidents touchant les données, incluant un mécanisme de signalement des incidents
- ☐ Accès à distance aux réseaux de l'organisation
- ☐ Élimination des actifs informatiques, des dispositifs et des données (y compris une politique en matière de conservation des données)
- ☐ Poursuite des activités et reprise après sinistre

UTILISATION ACCEPTABLE DES ACTIFS INFORMATIQUES

- ☐ L'organisation possède-t-elle des politiques en langage clair sur l'utilisation acceptable par les employés des systèmes et actifs d'information, du courriel et des autres services de communications, d'Internet, des appareils, etc.?
- ☐ La politique de l'organisation explique-t-elle l'utilisation acceptable des médias sociaux à des fins professionnelles et/ou l'échange autorisé de messages concernant l'organisation sur les médias sociaux?
- ☐ L'organisation possède-t-elle une politique sur l'utilisation d'équipement personnel de communication (« BYOD ») à des fins professionnelles?
- ☐ L'organisation possède-t-elle une politique sur le travail à domicile/télétravail et l'utilisation d'appareils mobiles et/ou de supports de stockage de données portables (clés USB, disques durs portables, etc.)?

SENSIBILISATION ET FORMATION DU PERSONNEL

- ☐ L'organisation publie-t-elle des politiques officielles sur la formation régulière du personnel, et tient-elle un registre des employés qui ont suivi et réussi cette formation?
- ☐ La formation a-t-elle lieu à l'accueil des nouveaux employés, au moment des changements de poste, et/ou sur une base régulière, et/ou en cas de révision importante d'une politique? Est-elle documentée, et/ou les employés doivent-ils attester qu'ils l'ont suivie et réussie? Les employés qui quittent l'organisation reçoivent-ils un rappel de leurs obligations en matière de retour des actifs informationnels?

CONTRÔLE PRÉALABLE DES FOURNISSEURS

- ☐ L'organisation possède-t-elle une politique établissant les critères normaux et suffisants de contrôle préalable de tous les fournisseurs qui auront accès à ses systèmes informatiques?

(Pour les fournisseurs de biens ou de services informatiques, le contrôle préalable qui déterminera la négociation et l'application des modalités relatives à la cybersécurité de leur contrat est important, et il est traité plus en détail ci-après, dans l'encadré intitulé « Exemples de contrôles préalables du fournisseur ».)

En cas d'atteinte à la protection des données, l'organisme de réglementation et, s'il y a poursuite, l'avocat du demandeur demanderont probablement à obtenir les politiques de l'organisation. Il serait donc judicieux que l'avocat-conseil examine toutes les politiques avant leur rédaction définitive.

Accès des tiers et ententes de services TI

Les privilèges d'utilisateur constituent les contrôles d'accès les plus simples. Il s'agit de droits accordés à un utilisateur pour lui permettre d'accéder aux systèmes et aux données de l'entreprise. Le principe le plus répandu est celui du « moindre privilège », par lequel l'utilisateur ne reçoit que le niveau d'accès nécessaire pour s'acquitter de ses fonctions.

Ce principe s'applique non seulement aux employés, mais aussi aux fournisseurs et aux autres tiers. Souvent, les relations de ce type sont régies par des contrats, qui peuvent aussi devenir des éléments clés de la préparation aux risques liés à la cybersécurité en établissant les dispositions relatives à la prévention, à l'atténuation et à la résolution des risques.

EXEMPLES DE FACTEURS D'ÉVALUATION DU PROFIL DE RISQUE EN MATIÈRE DE CYBERSÉCURITÉ D'UNE ORGANISATION

- L'organisation évolue-t-elle dans un secteur où un **cadre réglementaire** dicte les mesures de cyberprotection? Par exemple, dans le secteur des services financiers au Canada, l'entente devra respecter les règlements existants et émergents promulgués par le BSIF, l'OCRCVM et les ACVM.
- L'organisation fait-elle affaire dans **plusieurs juridictions?** Où les données sont-elles recueillies, traitées et stockées?
- S'agit-il d'une société fermée, ou d'une société ouverte comportant de **nombreux actionnaires** et assujettie à un contrôle des échanges?
- Des **renseignements personnels ou données médicales personnelles** seront-ils traités? Le cas échéant, il faudra tenir compte des lois sur la protection de la vie privée.
- La solution TI servira-t-elle au commerce de type **B2B ou B2C?**
- La solution TI prévoit-elle l'intervention de tiers comme des **fournisseurs de services d'hébergement ou de paiement**?
- L'organisation **conserve-t-elle ses données** sur place, dans un centre de données local ou dans le nuage?

On rencontre deux scénarios contractuels habituels : celui de la prestation directe de services TI ou celui de la fourniture d'un produit ou service qui exigera que le fournisseur accède aux systèmes informatiques (par exemple, un fournisseur de services d'éclairage doit accéder aux systèmes de contrôle environnemental des locaux de l'organisation). Un contrôle préalable raisonnable est nécessaire dans les deux cas, mais plus approfondi dans le premier.

Pour un contrat de services TI, le point de départ est la détermination des risques liés à la cybersécurité (voir ci-contre).

De plus, un contrôle préalable adéquat du fournisseur est essentiel pour conclure le meilleur contrat possible. La structure et les éléments de la solution proposée, ainsi que les capacités, les certifications, les pratiques de gestion des risques et les ressources financières du fournisseur, sont tous des éléments à explorer (voir ci-contre).

Un fois le profil de risque en matière de cybersécurité de l'organisation établi, et un contrôle préalable rigoureux du fournisseur effectué, l'équipe des services juridiques est en mesure d'adapter l'entente de services TI proposée en fonction des dispositions applicables sur la prévention, l'atténuation et la résolution des atteintes à la protection des données.

Certaines des plus importantes dispositions de l'entente concernent la répartition des risques. L'influence réciproque des déclarations, des garanties, des indemnisations et des responsabilités est en général fortement contestée dans le domaine de la cybersécurité, car la jurisprudence évolue sans cesse. Une organisation aura intérêt à consulter des avocats externes expérimentés dans ce domaine pour déterminer comment il convient d'aborder ces questions et pour explorer les diverses avenues possibles.

EXEMPLES DE CONTRÔLES PRÉALABLES DU FOURNISSEUR

- Quel est le **cadre de sécurité** du fournisseur? Quelles politiques et procédures sont en place pour en assurer l'intégrité?
- Le fournisseur autorisera-t-il les **essais de pénétration** et l'exploration d'autres vulnérabilités?
- Les installations du fournisseur sont-elles vérifiées en fonction de contrôles internes reconnus? Le fournisseur procède-t-il à des **audits internes**, et est-il prêt à en communiquer les résultats au client?
- Où se trouvent les centres de service du fournisseur? Où les **données** sont-elles traitées et **stockées?**
- À quelle assurance contre les cyberrisques le fournisseur souscrit-il, et a-t-il présenté des **demandes d'indemnité** au cours des cinq dernières années?
- Le fournisseur respecte-t-il les **normes de sécurité** reconnues dans l'industrie (y compris, s'il y a lieu, celles qui concernent l'informatique en nuage)?

Sécurité des TI, logiciels malveillants et surveillance

Les défenses TI de l'organisation constituent un aspect vital de la gestion des risques – sont-elles adéquates, à jour et adaptées aux menaces connues? Il est important que l'organisation s'abonne à un service d'évaluation des menaces exhaustif et légitime (les bulletins sur la cybersécurité et les documents sur les meilleures pratiques du Centre canadien de réponse aux incidents cybernétiques (CCRIC), par exemple)[9]. Il existe aussi des groupes d'industrie et sectoriels voués au partage de l'information. À titre d'exemple, le Comité sur les paiements et les infrastructures de marché de la Banque des règlements internationaux a publié

9 Ressources du Centre canadien de réponse aux incidents cybernétiques, en ligne à l'adresse <http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-eng.aspx>.

un rapport sur les pratiques de cybersécurité actuelles des institutions financières[10].

La Banque du Canada a adopté la norme conseillée par le Comité en matière de gestion des risques pour les institutions financières désignées, soulignant que les « projets de coopération qui facilitent la mise en commun de l'information renforcent la cybersécurité en créant un espace de discussion propice à l'échange de pratiques exemplaires et de renseignements sur les menaces, ainsi qu'à l'établissement de réseaux de confiance intersectoriels[11] » .

Une organisation doit donc installer des logiciels standards de protection contre les virus et les maliciels, et en assurer la mise à jour régulière et documentée, protéger ses réseaux, y compris les réseaux sans fil, contre les attaques internes et externes au moyen de méthodes normalisées, comme des pare-feu et des systèmes de détection continuelle des logiciels malveillants, procéder régulièrement à des essais de pénétration (idéalement exécutés par un tiers indépendant) et mettre en place des solutions techniques de détection et de blocage des activités ou des accès suspects.

Les attaques d'ingénierie sociale doivent aussi être envisagées, et les organisations devraient penser à former leurs employés sur les façons d'éviter d'être victime d'hameçonnage, sur les dangers des « mauvais jumeaux » (points d'accès Wi-Fi illicites qui semblent être des points

10 « Cyber resilience in financial market infrastructures », Committee on Payments and Market Infrastructures, novembre 2014, en ligne à l'adresse <http://www.bis.org/cpmi/publ/d122.pdf>.

11 « Résilience du système financier canadien : l'apport de la cybersécurité », Banque du Canada, décembre 2014, en ligne à l'adresse <http://www.bankofcanada.ca/wp-content/uploads/2014/12/fsr-december14-morrow.pdf>.

RENSEIGNEMENTS PERSONNELS

Ce qui est couvert

Les lois canadiennes sur la protection de la vie privée ne s'appliquent qu'aux **renseignements personnels**, définis au sens large comme des renseignements sur un particulier identifiable.

On considère qu'un renseignement porte « sur » un **« particulier identifiable »** s'il est très possible qu'une personne puisse être identifiée au moyen de ce renseignement, seul ou combiné à d'autres renseignements. Soulignons que le terme « renseignement personnel » se prête à une interprétation large et qu'il s'applique notamment aux adresses IP, aux enregistrements vocaux et aux coordonnées.

Veuillez noter qu'aux termes de la loi, un renseignement est considéré comme personnel même s'il est de **nature publique.**

Ce qui n'est pas couvert

Aux termes de la **LPRPDE**, le nom et le titre d'un employé d'une organisation ainsi que les adresse et numéro de téléphone de son lieu de travail ne constituent pas un renseignement personnel. Fait à noter, dans la loi fédérale, cette exception ne touche pas l'adresse courriel d'entreprise, qui est considérée comme un renseignement personnel. De plus, cette exception ne figure pas dans la loi de certaines provinces (la Loi sur la protection des renseignements personnels du Québec, par exemple).

De plus, la LPRPDE ne s'applique qu'aux organisations qui recueillent, utilisent et communiquent des renseignements personnels **« dans le cadre d'activités commerciales ».**

La LPRPDE ne s'applique pas aux **employés du secteur privé,** qui peuvent toutefois être régis par d'autres lois provinciales sur la protection de la vie privée.

d'accès légitimes offerts sur place, mais qui en réalité ont été créés par des pirates pour intercepter les communications sans fil; les utilisateurs bernés connectent leur ordinateur portable ou téléphone mobile au point d'accès frauduleux du pirate, qui se présente comme un fournisseur légitime) et sur les clés USB qui semblent avoir été égarées, mais qui en fait ont été délibérément infectées par un logiciel malveillant et laissées sur place.

Cyberassurance

Alors que le nombre, la portée et l'impact des atteintes à la sécurité des données ne cessent d'augmenter, les organisations cherchent à transférer les risques connexes, le plus souvent en obtenant une police d'assurance : si le risque est assurable, il est transférable. Marsh Inc., courtier d'assurance d'envergure mondiale, affirme que le nombre d'organisations ayant acheté une cyberassurance aux États-Unis a augmenté de 33 % entre 2011 et 2012, et que le secteur de l'assurance commerciale dont l'expansion est la plus rapide au monde est celui des cyberassurances[12].

En général, une assurance contre les risques liés à la cybersécurité offre deux protections : une couverture des pertes directes du titulaire de la police et une couverture d'assurance responsabilité qui protège des réclamations de tiers.

COUVERTURE DES RISQUES PROPRES AU TITULAIRE :
☐ Coûts associés à la détermination de la portée d'un incident et aux mesures palliatives
☐ Coûts des avis aux personnes dont les renseignements personnels ont été compromis
☐ Services de relations publiques pour contrecarrer la publicité négative pouvant découler d'une enquête
☐ Coûts de réponse aux enquêtes du gouvernement
☐ Coûts de remplacement du matériel ou des logiciels endommagés
☐ Coûts d'intervention face au vandalisme des données électroniques de l'entreprise
☐ Coûts de l'interruption des activités d'affaires

12 « Companies turn to cyber insurance after Ashley Madison and other high-profile hacks », CBC News, 14 octobre 2015, en ligne à l'adresse http://www.cbc.ca/news/canada/kitchener-waterloo/companies-turn-to-cyber-insurance-after-ashley-madison-and-other-high-profile-hacks-1.3270756.

COUVERTURE D'ASSURANCE RESPONSABILITÉ ENVERS LES TIERS :
☐ Responsabilité à l'égard de l'accès aux renseignements personnels des clients
☐ Transmission d'un virus ou d'un logiciel malveillant à un client ou à un partenaire d'affaires
☐ Défaut d'aviser un tiers de ses droits en vertu de la réglementation pertinente en cas d'atteinte à la protection des données
☐ Possibles préjudices imputables à la publicité (par les médias électroniques, tels que l'utilisation non autorisée ou la contrefaçon d'œuvres protégées par le droit d'auteur ainsi que les poursuites pour diffamation, calomnie et atteinte à la réputation)

Une assurance contre les risques liés à la cybersécurité peut aussi couvrir la crise suivant une atteinte à la protection des données, notamment les frais liés à la gestion de l'incident (enquête, mesures correctives, avis obligatoires, établissement d'un centre d'appel, gestion des relations publiques, vérifications de crédit des personnes concernées) et les frais juridiques (amendes ou frais de poursuite ou de défense).

Toute couverture d'assurance est subordonnée aux modalités de la police. Les organisations doivent donc se poser quelques questions et faire examiner leur police par un conseiller en la matière.

EXEMPLES DE QUESTIONS RELATIVES À UNE CYBERASSURANCE :
☐ Quels contrôles de sécurité peut-on mettre en place pour réduire la prime?
☐ Faudra-t-il se soumettre à un quelconque examen des risques de sécurité?
☐ Qu'attend-on de l'organisation en matière de réduction ou de limitation des risques?
☐ L'assureur accorde-t-il un rabais pour les années sans réclamation?
☐ Peut-on présenter une demande de règlement si une intrusion n'est détectée que des mois ou des années plus tard, soit hors de la période de couverture?
☐ Qui prend la décision de payer ou de ne pas payer la rançon?

Plan d'intervention

Jusqu'à présent, nous avons orienté la discussion sur les éléments proactifs d'un plan de cybersécurité. Un autre aspect important d'un programme de cybersécurité est le plan d'intervention réactif.

L'efficacité d'un plan d'intervention en cas d'incident dépend au bout du compte de l'appui de la direction. L'étape suivante dans l'élaboration d'un plan d'intervention efficace consiste à réunir la bonne équipe. Le plan d'intervention doit s'appliquer à l'échelle de l'entreprise et mettre à profit l'expérience d'une équipe de représentants des principales parties prenantes au sein de l'organisation. Habituellement, elle sera formée de cadres supérieurs des services juridiques, des relations publiques et du marketing, du service à la clientèle, des ressources humaines, de la gestion de la sécurité/des risques de l'entreprise et des TI. Idéalement, des conseillers externes préexaminés et présélectionnés seront également impliqués.

Les responsabilités de l'équipe et les détails du plan font l'objet de la partie IV ci-après.

Une fois le plan d'intervention rédigé, il ne doit pas reposer dans un tiroir. Les organisations doivent former et exercer leur personnel et procéder à des simulations d'incidents afin de développer des automatismes. Celles qui se préparent le mieux mènent régulièrement des simulations de crise pour mettre leurs plans à l'épreuve, augmenter la sensibilisation des dirigeants et perfectionner leurs capacités d'intervention. De plus, elles invitent souvent un conseiller externe expérimenté, pour avoir traité des dizaines d'incidents, à participer à la simulation afin d'évaluer la réaction de l'organisation.

PARTIE IV: EXÉCUTION EFFICACE DU PLAN D'INTERVENTION

Que faire durant les 72 premières heures.

Un plan d'intervention détaillé doit être préparé en avance, testé, et bien compris des membres de l'organisation. Il aidera un groupe diversifié à concerter efficacement ses efforts en cas de crise et préviendra les communications bien intentionnées, mais mal coordonnées (tant à l'interne qu'à l'externe).

Les parties prenantes de toute l'entreprise doivent être consultées pour l'élaboration du plan d'intervention. Chacune d'elle devra désigner parmi leur groupe un responsable pour a) l'exécution des dispositions du plan qui touchent le groupe; et b) assurer les suivis auprès de la direction.

Plusieurs étapes reconnues doivent faire partie du plan d'intervention :

1. Contenir les effets de l'incident

Les atteintes à la protection des données ne sont pas toutes le fait de redoutables pirates qui s'attaquent aux systèmes informatiques des organisations. Les incidents physiques (qui ne sont pas d'origine électronique, comme un employé qui quitte l'entreprise en emportant des renseignements avec lui, la perte de dossiers ou d'appareils et le vol d'ordinateurs portables) sont toujours monnaie courante. Soulignons que le plan d'intervention de l'organisation ne doit pas s'appliquer seulement en cas de brèche électronique, mais aussi en cas d'incident physique critique.

En fonction de la nature et de la portée de l'incident physique, il peut convenir ou ne pas convenir

DÈS LA DÉCOUVERTE

DÉCOUVERTE	Consignez **la date, l'heure, le lieu et la durée de l'incident** (était-ce une intrusion ponctuelle ou un logiciel malveillant en place depuis des mois?). Documentez la façon dont la brèche a été découverte, etpar qui.
BRÈCHE	Documentez **les détails entourant l'incident** (point d'entrée, méthode d'intrusion, systèmes affectés, accès à des renseignements, données supprimées, modifiées ou volées).
DONNÉES	Documentez les **détails relatifs aux données compromises**. Qui sont les personnes touchées (des clients ou des employés)? Où se trouvent **les personnes touchées**? Quels sont les **types de renseignements compromis** (s'agit-il de renseignements personnels ou d'autres données)? Les renseignements sont-ils cryptés? Combien d'enregistrements sont touchés?

S'il y a lieu, commencez immédiatement à inscrire la mention « Privilégié et confidentiel. Préparé sous la direction d'un conseiller juridique en prévision d'un litige. » sur tous les rapports écrits et autres documents produits.

d'exécuter le plan et de réunir l'équipe d'intervention. Quelle que soit la situation, la première chose à faire est de lancer une enquête et d'agir rapidement pour limiter la perte des données. Pour ce faire, on peut restreindre l'accès des employés et du public aux secteurs touchés et, au besoin, remplacer les serrures et les cartes d'accès. L'organisation doit déterminer s'il est nécessaire d'aviser la police. Si une enquête interne ou externe est en cours, il faudra notamment dresser la liste des actifs perdus ou affectés, obtenir les renseignements de suivi et les vidéos de surveillance disponibles (le cas échéant) et, si l'incident implique l'inconduite d'un employé, envisager les conséquences de cette enquête du point de vue des RH.

En cas d'incident électronique (un piratage ou une autre atteinte à l'infrastructure des TI ayant entraîné la perte de données ou une infiltration, par exemple), il est probable que les dégâts soient plus difficiles à contenir et que l'organisation doive mettre en œuvre son plan et réunir l'équipe d'intervention. La décision dépendra en grande partie de l'importance de l'incident et du type de renseignements touchés.

2. Réunir l'équipe

S'il y a lieu, il faut communiquer avec les membres de l'équipe, les réunir et les mettre au courant de la situation. L'utilisation du téléphone seulement (et, dans certains cas, de nouveaux téléphones mobiles) pourrait être nécessaire afin d'éviter l'utilisation d'un système de courriel compromis et, de ce fait, les fuites. Des canaux de communication sécurisés (téléphones, ordinateurs portables, réseaux) doivent également être mis à la disposition de la haute direction et d'autres employés clés.

Une fois le plan d'intervention amorcé, les canaux de communication, les structures de signalement et les responsabilités devraient être clairs. Au moment de décider de ces canaux et structures, il est essentiel d'avoir déjà envisagé la manière la plus efficace pour faire intervenir les conseillers juridiques internes et externes afin de préserver le secret professionnel (le cas échéant).

La composition de l'équipe peut varier en fonction de l'organisation et de la nature de l'incident, mais ses responsabilités seront généralement les suivantes :

SERVICES JURIDIQUES/CONFORMITÉ
☐ Mettre en œuvre, avec un conseiller juridique externe, un protocole de préservation du secret professionnel
☐ Déterminer comment aviser les personnes touchées, les médias, la police, les organismes de réglementation gouvernementaux et autres tiers (émetteurs de cartes de crédit, banques, etc.)

- ☐ Établir des relations avec un conseiller juridique externe avant qu'un incident se produise et gérer les services-conseils externes pendant l'intervention
- ☐ Gérer l'ensemble des avis statutaires dans toutes les juridictions ainsi que les communications 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 sous la direction d'un conseiller juridique
- ☐ Émettre un avis de préservation en cas de litige et en assurer le suivi
- ☐ Gérer l'information et dresser la liste des personnes à informer
- ☐ Passer en revue les communications sortantes, les déclarations, les rapports, etc.

RELATIONS PUBLIQUES/MARKETING

- ☐ Se renseigner sur les réseaux et les acteurs du secteur d'activité et, avant qu'un incident se produise, établir les principales stratégies de relations avec les médias
- ☐ Élaborer un plan de communication interne, qui met l'accent sur la confidentialité et les mesures que les employés doivent prendre si les médias communiquent avec eux, et un plan d'intervention en cas de fuite de renseignements sur l'incident
- ☐ Assurer le suivi de la couverture médiatique et l'analyser, et établir un plan d'intervention en cas de couverture négative, au besoin

SERVICE À LA CLIENTÈLE

- ☐ Dresser une liste d'arguments afin de déterminer s'il faut mener les enquêtes sur l'incident à l'interne ou mettre en place un centre d'appel
- ☐ Mettre en place un centre d'appel et un programme de protection du consommateur (voir ci-après et l'encadré « Centres d'appel » pour plus d'information)
- ☐ Traiter les plaintes de clients

RESSOURCES HUMAINES

- ☐ Gérer les employés pendant l'incident, incluant la réaffectation de ressources humaines, au besoin

☐	Gérer les enquêtes, les mesures disciplinaires et la cessation d'emploi, si l'incident est attribuable à un acte répréhensible d'un employé

GESTION DE LA SÉCURITÉ/DES RISQUES DE L'ENTREPRISE	
☐	Communiquer avec les forces de l'ordre (avec les services juridiques), y compris la GRC et peut-être le SCRS, le CSTC, le FBI et les services secrets, lorsque l'incident est de grande envergure
☐	Communiquer les directives des forces de l'ordre à l'équipe, et veiller à ce qu'elles soient respectées
☐	Gérer les risques liés à l'incident, l'isolement des secteurs touchés et les accès physiques

TI	
☐	Collaborer avec des spécialistes externes de l'informatique judiciaire au repérage et à l'élimination des programmes malveillants ou d'autres artefacts utilisés pour commettre une attaque, si cette dernière est d'origine électronique
☐	Participer à la collecte de preuves, à la gestion des avis de préservation et aux poursuites judiciaires

3. Analyser l'incident

L'organisation doit commencer à recueillir de l'information dès qu'un incident est signalé. Tous les renseignements sur l'incident doivent faire l'objet d'un avis de préservation exhaustif de sorte qu'ils soient conservés, recueillis et analysés sous la direction d'un conseiller juridique (et transmis aux forces de l'ordre, au besoin). Des avocats les étudieront ensuite pour déterminer quels renseignements seront pertinents en cas de poursuite, mais il faut d'abord recueillir et préserver tous les renseignements qui pourraient l'être.

Lorsque la cause de l'incident aura été identifiée, et qu'on aura déterminé les personnes touchées, l'organisation sera en mesure de prévoir comment l'information compromise pourrait être utilisée (était-ce des renseignements financiers personnels non cryptés qui étaient visés par une attaque malveillante? Ou a-t-on seulement perdu une clé USB non cryptée contenant des noms et des adresses? Dans le premier cas, les renseignements sont beaucoup plus susceptibles d'être vendus sur des marchés noirs en ligne et utilisés pour une fraude ou un vol d'identité.) L'organisation

peut alors commencer à prendre des décisions pour atténuer les risques, protéger les consommateurs et faire respecter la loi, entre autres.

En cas d'incident, l'organisation dispose de peu de temps pour recueillir d'importants éléments de preuve. Bien que les membres de l'équipe interne des TI agissent comme premiers intervenants, il arrive souvent qu'ils ne soient pas qualifiés en récupération de données et en analyse judiciaire, et ils font parfois plus de mal que de bien en endommageant des données critiques ou en manipulant par erreur des éléments de preuve importants de façon inadéquate. Pour cette raison, un cabinet externe d'informatique judiciaire, qui utilise des logiciels et des protocoles d'informatique judiciaire pour recueillir et préserver les données à la suite d'un incident, devrait être parmi les premiers fournisseurs dont on retient les services après une atteinte à la sécurité.

COMPÉTENCES DU CABINET D'INFORMATIQUE JUDICIAIRE
☐ Être en mesure de repérer et de neutraliser la menace tout en préservant et en manipulant les éléments de preuve au moyen d'une méthode éprouvée et efficace sur le plan judiciaire, ainsi que d'outils et de processus de récupération de données reconnus par la jurisprudence et le fruit de son expérience en litige
☐ Pouvoir travailler avec des systèmes d'exploitation et des appareils diversifiés (pas seulement des ordinateurs, mais aussi des ordinateurs portables, des appareils mobiles, des systèmes de localisation GPS et, dans bien des cas, des technologies dépassées toujours en usage)
☐ Savoir accomplir des tâches critiques en ménageant les susceptibilités, dans le respect de la culture du lieu de travail, car le cabinet devra poser des questions aux employés et accéder à leur poste de travail et à leurs appareils (ainsi qu'à leurs appareils personnels, dans certains cas), au moins temporairement
☐ Pouvoir former une équipe dont les membres ont l'expérience nécessaire à l'assistance d'un conseiller interne ou externe à constituer un dossier
☐ Trouver des personnes clés pouvant témoigner de façon convaincante devant le tribunal
☐ Bien comprendre les questions liées au secret professionnel et les avis de préservation, savoir les gérer et comprendre le rôle que les enquêtes et les rapports peuvent jouer ultérieurement devant les instances réglementaires et les tribunaux

Les organisations doivent avoir établi ces relations avant qu'un incident se produise et, idéalement, avoir déjà coordonné l'intervention avec le conseiller juridique externe sélectionné afin d'assurer un transfert harmonieux en cas d'incident réel.

4. Évaluer et gérer les conséquences juridiques

Pendant que les renseignements sont recueillis et préservés, et que la nature et la portée de l'incident se précisent, l'organisation doit également réfléchir (même à cette étape précoce de l'intervention) au risque de litige à moyen et à long terme découlant de l'incident.

RISQUE DE LITIGE – ACTIONS COLLECTIVES

À la suite d'un incident important relatif aux données, il est presque inévitable qu'un ou peut-être deux types d'actions collectives soient dirigées contre l'organisation. Premièrement, une action collective de consommateurs sera presque assurément exercée au nom de tous les clients potentiellement touchés par la fuite de renseignements personnels. Deuxièmement, si l'organisation est un émetteur public canadien dont le cours de l'action a chuté juste après l'annonce de l'incident, elle pourrait être poursuivie par un représentant des actionnaires au motif que ses documents d'information continue sur l'état des systèmes de cybersécurité étaient trompeurs.

Au moment où ces lignes ont été écrites, aucune action collective dans le secteur des valeurs mobilières n'avait été intenté au Canada à la suite d'un incident, mais plusieurs actions collectives de consommateurs ont été intentés. Les tribunaux canadiens n'ayant pas terminé de se prononcer sur ces dossiers, les questions relatives à la validité juridique des causes d'actions invoquées et la portée des possibles dommages-intérêts demeurent très incertaines[13].

13 Dans le cas d'une action collective intentée devant un tribunal provincial, l'existence de causes d'action en vertu de la common law ou de la loi dépend du territoire. Selon la loi sur la protection de la vie privée de la Colombie-Britannique, par exemple, il y a délit d'atteinte à la vie privée si une personne, intentionnellement et sans apparence de droit, porte atteinte à la vie privée d'autrui. Ce délit donne un droit d'action sans qu'il soit nécessaire de prouver un dommage. Par conséquent, dans cette province, il est communément admis qu'il n'y a pas de délit particulier d'atteinte à la vie privée reconnu en common law, et les demandes en common law peuvent donc être rejetées. Une règle d'exclusion semblable s'applique à l'Alberta. Quant à la Cour fédérale, elle a conclu que la procédure énoncée dans la LPRPDE constitue le seul recours pour déposer une plainte pour atteinte à la vie privée relevant du secteur privé, bien qu'une cause d'action pour atteinte à la vie privée en vertu de la common law n'ait pas été rejetée dans une action collective intentée contre le gouvernement fédéral. En revanche, en Ontario, la Cour d'appel a confirmé dans l'arrêt *Jones c. Tsige* l'existence d'un délit d'atteinte à la vie privée en common law qui s'applique aux renseignements personnels généraux. La jurisprudence continue à évoluer à tous égards.

Au Canada, les actions collectives de consommateurs ou d'actionnaires sont presque toujours intentées devant un tribunal provincial (et non fédéral). Une seule action collective peut être intentée par province, et les cabinets demandeurs tiennent généralement pour acquis qu'ils sont les premiers à présenter une demande dans la province, ce qui prévient les poursuites concurrentes sur un même territoire. Par conséquent, les cabinets demandeurs intentent généralement une poursuite à la suite d'une atteinte à la protection des données dès qu'ils trouvent un représentant convenable qui pourrait avoir été touché. Souvent, la formulation de la demande introductive d'instance est générique et ne contient que le nom de l'organisation et une description sommaire de l'incident. Il est probable qu'aucune enquête sur le fond ne soit menée avant le dépôt de l'action collective proposée (généralement accompagnée d'un communiqué de presse).

En général, l'organisation peut s'attendre à ce que la première poursuite soit intentée dans les 7 à 30 jours. Si deux mois s'écoulent sans poursuite, la probabilité d'action en justice diminue considérablement (à moins que d'autres renseignements importants sur l'incident ne soient communiqués, par exemple en ce qui a trait au nombre de personnes touchées, au type de renseignements compromis ou au dévoilement d'allégations de fraude plausibles en lien avec l'incident).

Au Canada, il est possible de déposer des actions collectives concurrentes dans diverses provinces. Par conséquent, une organisation peut avoir à se défendre dans plusieurs causes parallèles simultanées. Qu'il y en ait une ou plusieurs, les actions collectives ont tendance à progresser lentement (surtout si on continue à découvrir de nouveaux faits; par ailleurs, les lois sur la responsabilité et les dommages-intérêts, là encore, ne sont pas claires). De trois à cinq années peuvent s'écouler avant qu'une action collective fasse l'objet d'une décision ou d'un règlement. Pour cette raison, l'organisation devrait compter un expert en litiges externe dans son équipe de cybersécurité et le mettre au courant dès que possible; ce conseiller s'occupera des conséquences à long terme (en invoquant le secret professionnel, en lisant les messages d'information publique, etc.) pendant que l'organisation et ses ressources se concentreront sur l'intervention immédiate.

RISQUE RÉGLEMENTAIRE

L'organisation peut également s'attendre à être visée par des procédures réglementaires. Il s'agira principalement d'une enquête menée par divers commissaires à la protection de la vie privée, de leur propre initiative ou à la suite de plaintes, et, selon le secteur d'activité, par des organismes de réglementation des valeurs mobilières, des institutions financières ou des organismes de réglementation de la santé publique, voire même les forces de l'ordre.

Commissaires à la protection de la vie privée

En matière de protection de la vie privée, les principaux organismes de réglementation sont les divers commissaires à la protection de la vie privée provinciaux et le commissaire à la protection de la vie privée du Canada. L'une des principales responsabilités d'une organisation victime d'une atteinte à la protection des données mettant en jeu des renseignements personnels est d'aviser ces divers commissaires.

La loi peut obliger les organisations à aviser les organismes de réglementation ou les personnes concernées. Pour l'instant, seuls l'Alberta et le Manitoba ont adopté une loi rendant obligatoire le signalement des brèches de sécurité dans le secteur privé, à l'exception du secteur de la santé (la loi du Manitoba n'était pas encore entrée en vigueur au moment d'écrire ces lignes). Les modifications apportées à la LPRPDE en raison de la *Loi sur la protection des renseignements personnels numériques* rendent maintenant obligatoire de notifier les personnes touchées et le commissaire à la protection de la vie privée du Canada, mais les articles pertinents n'entreront en vigueur qu'après l'adoption des règlements d'application. Dans le secteur de la santé, l'Alberta, l'Ontario, Terre-Neuve-et-Labrador et le Nouveau-Brunswick ont tous adopté des lois qui exigent le signalement des brèches de sécurité.

Le défaut de signaler une atteinte à la protection des données peut mener à des sanctions. En Alberta, dans le secteur privé, le signalement est obligatoire « s'il est raisonnable de croire, dans les circonstances, que l'atteinte présente un risque réel de préjudice grave à l'endroit d'un individu». L'omission de signaler au commissaire à la vie privée de l'Alberta une brèche présentant un risque réel de préjudice grave aux intéressés constitue une infraction passible d'une amende d'au plus 10 000 $ pour un particulier et d'au plus 100 000 $ pour une entreprise.

En pratique, l'organisation avise généralement tous les commissaires à la protection de la vie privée concernés (que le signalement soit obligatoire ou non) au moyen d'un processus de signalement coordonné garantissant la cohérence de l'information. Les organisations doivent savoir que bien que les renseignements transmis à un commissaire à la protection de la vie privée demeurent généralement confidentiels, certains pourraient devoir être divulgués ultérieurement à la suite de demandes en vertu des lois sur l'accès à l'information.

Les plaintes personnelles déposées auprès d'un commissaire à la protection de la vie privée déclenchent des enquêtes visant à résoudre la question en litige, mais un commissaire peut également amorcer de sa propre initiative une enquête sur une question relevant de sa compétence. Il est plus probable qu'une enquête soit menée si les plaintes personnelles sont nombreuses, si l'incident est de grande envergure ou touche des renseignements particulièrement critiques, si les politiques publiques sont au cœur d'un enjeu important ou doivent faire l'objet d'une réorientation (en raison de l'apparition d'un nouveau type de service ou d'un nouveau modèle d'affaires, par exemple), ou si 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 l'intervention de l'organisation.

NOUVELLES MESURES INTRODUITES DANS LA LPRPDE

La Loi sur la protection des renseignements personnels numériques (projet de loi S-4)

En juin 2015, la *Loi sur la protection des renseignements personnels numériques* a introduit de nouvelles mesures dans la LPRPDE. Ces mesures et améliorations sont **aujourd'hui en vigueur**, excepté celles concernant les exigences à l'égard des atteintes à la protection des données dont il est question ci-dessous, qui attendent l'adoption des règlements connexes.

Signalement obligatoire d'une atteinte : Bien qu'elles ne soient pas encore en vigueur, ces nouvelles dispositions obligent les organisations à déclarer une atteinte à la protection des données tant aux personnes touchées qu'au Commissariat à la protection de la vie privée (le « commissaire »), et ce, en respectant certaines conditions. Ces dispositions prévoient notamment que les organisations doivent déclarer au commissaire toute atteinte aux mesures de sécurité qui a trait à des renseignements personnels dont elles ont la gestion, s'il est raisonnable de croire, dans les circonstances, que l'atteinte présente un risque réel de préjudice grave à l'endroit d'un individu. La déclaration doit être faite « le plus tôt possible après que l'organisation a conclu qu'il y a eu atteinte ».

La Loi définit longuement un « risque réel de préjudice grave », qui comprend notamment « 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 exhaustive d'un préjudice, combinée à l'exigence de déclaration « le plus tôt possible », soulève de nouvelles questions et impose un nouveau fardeau aux organisations.

De plus, une organisation visée par une atteinte devra aviser toute autre organisation ou toute institution gouvernementale si elle croit que celle-ci peut être en mesure de réduire le risque de préjudice pouvant résulter de l'atteinte.

Compte tenu de ces lourdes obligations à l'égard des atteintes à la sécurité, il est impératif qu'une organisation retienne les services d'un conseiller juridique externe dès la détection d'une brèche afin de satisfaire amplement l'exigence de déclaration au plus tôt, car son non-respect peut entraîner de sévères sanctions.

Sanctions : La Loi impose une responsabilité à quiconque contrevient sciemment aux exigences d'avis. Une organisation peut donc s'exposer à des amendes pouvant aller jusqu'à 100 000 $ CA par infraction.

Confidentialité : La Loi accorde au commissaire le droit de rendre publique toute information qu'il obtient dans le cadre de l'exercice de ses devoirs ou de ses pouvoirs, de même que le contenu des avis d'atteinte aux mesures de sécurité qui lui sont transmis, ce qui va bien au-delà du pouvoir doit il jouissait déjà en vertu de la LPRPDE de montrer du doigt les contrevenants.

Prises ensemble, ces dispositions imposent aux organisations des obligations plus strictes en matière de protection des renseignements personnels, de consentement et de déclaration d'atteinte à la sécurité. Les organisations doivent continuer de trouver un équilibre entre ces nouvelles obligations et la nécessité de réduire au minimum les frais financiers et les coûts d'une atteinte à la réputation résultant d'une fuite de données. La Loi rend cet exercice de conciliation encore plus compliqué, les coûts de non-conformité encore plus élevés et le besoin d'un plan d'intervention réfléchi encore plus impérieux.

OBLIGATIONS RELATIVES AUX CARTES DE PAIEMENT ET À LA NORME PCI DSS

Les incidents relatifs aux cartes de paiement ou qui se traduisent par la perte de renseignements sur leurs détenteurs ou l'accès non autorisé à ces renseignements soulèvent des questions particulières liées à la complexité des réseaux de paiement et des diverses relations contractuelles entre leurs acteurs. En ce moment, au Canada, les lois et règlements ne rendent pas obligatoire le signalement des atteintes à la protection des données aux fournisseurs de cartes de paiement et aux banques acquéreuses, mais les divers contrats ayant trait à l'utilisation et à l'émission de cartes de paiement entre les organisations commerciales et les nombreux fournisseurs de cartes bancaires et de paiement pourraient tout à fait donner lieu à une telle obligation.

Des normes sectorielles peuvent s'appliquer. Le Conseil des normes de sécurité PCI a été fondé par de grands fournisseurs de cartes de paiement. Les organisations – y compris les acquéreurs, les fournisseurs de services et les commerçants – qui acceptent les paiements effectués au moyen d'une carte de n'importe lequel de ces fournisseurs doivent satisfaire aux exigences de la norme PCI DSS (Payment Card Industry Data Security Standard). Le Conseil des normes de sécurité a compétence exclusive pour fixer ces exigences, mais il ne participe pas à la vérification de la conformité. Ce sont les fournisseurs de cartes qui doivent eux-mêmes garantir la conformité des transactions effectuées avec leurs produits, en veillant à ce que les banques acquéreuses respectent leurs politiques. Ces dernières, à leur tour, s'assurent de la conformité des commerçants. Par conséquent, si une organisation souhaite accepter les cartes de crédit de grands fournisseurs, elle doit faire affaire avec les acquéreurs de ceux-ci, qui inscrivent des mesures de conformité à la norme PCI DSS dans leurs contrats de service.

La norme PCI DSS exige la rédaction et la tenue à jour de documents, l'application de contrôles de sécurité préventifs et de détection, et la mise en place de processus dans le but de repérer et de maîtriser les tentatives de brèches de sécurité aussi vite que possible. Un enquêteur judiciaire PCI (PFI), cabinet d'informatique judiciaire approuvé par les fournisseurs de cartes, vérifie périodiquement la conformité de l'organisation aux normes PCI DSS et produit des rapports pour recommander que la certification soit renouvelée ou refusée. Les organisations non conformes s'exposent à une hausse des frais de transaction par les banques acquéreuses, à des pénalités contractuelles imposées par les fournisseurs de cartes de paiement, à une responsabilité accrue en cas de brèche et au retrait de l'autorisation de traiter des transactions par carte de paiement.

D'autres avis peuvent être requis en fonction du secteur. En cas d'incident, l'organisation touchée doit souvent aviser ses banques acquéreuses et (ou) les fournisseurs de services de paiement concernés (conformément aux règles et aux exigences de l'industrie des cartes de paiement relatives aux acquéreurs, aux émetteurs et (ou) aux fournisseurs de cartes de paiement concernés), et elle peut être contractuellement tenue de faire appel à un PFI approuvé pour qu'il enquête sur la faille de sécurité, en détermine la cause et en fasse rapport aux fournisseurs de

services de paiement touchés et aux autres parties concernées. L'enquête du PFI est souvent menée parallèlement à l'enquête informatique de l'organisation.

La norme PCI DSS ne fournit pas de lignes directrices particulières pour la gestion d'une brèche de sécurité. Chaque fournisseur de cartes de paiement dispose de ses propres politiques et procédures; par exemple, certains exigent un signalement immédiat dès qu'une atteinte à la protection des données est confirmée, d'autres l'exigent dans les 24 heures.

On peut être tenté de retarder ou d'omettre ce signalement. Or, même si l'organisation ne les prévient pas, il est très probable que la banque et (ou) les membres du réseau de fournisseurs de cartes remontent jusqu'à elle en voulant déterminer l'origine de la compromission de données sur des détenteurs de cartes. Les banques et les fournisseurs de cartes de paiement ont mis en œuvre des processus visant à retracer la source d'un incident le plus précisément possible.

Un conseiller juridique doit participer à toutes les discussions avec les PFI et aux enquêtes connexes. L'organisation peut consulter un conseiller externe spécialiste du domaine pour déterminer la façon dont elle souhaite gérer l'enquête du PFI ainsi que ses interactions avec les fournisseurs de cartes, sa propre enquête informatique parallèle et la protection du secret professionnel. Les enjeux étant élevés et complexes, l'organisation aura avantage à gérer de manière stratégique les questions liées au secret professionnel.

DIVULGATION DU RISQUE PAR LES SOCIÉTÉS OUVERTES

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, ce qui comprend les prospectus et les documents d'information continue, comme les notices annuelles. Par exemple, les dispositions du règlement 51-102F1 (rapport de gestion) prévoient une analyse des risques qui ont eu une incidence sur les états financiers ou qui pourraient en avoir une ultérieurement, ainsi que des risques et incertitudes qui, d'après l'émetteur, auront une incidence importante sur la performance future.

Les ACVM ont publié l'Avis 2016, qui met à jour l'avis 11-326 précédent sur le même sujet (l'« Avis 2013 ») pour les émetteurs assujettis, les sociétés inscrites et les entités réglementées. Comme le mentionnent les ACVM, depuis la publication de l'Avis 2013, le contexte de la cybersécurité a considérablement évolué, les cyberattaques devenant plus fréquentes, complexes et coûteuses pour les organisations. Citant deux récentes études, les ACVM ont mentionné dans l'Avis 2016 ces deux constatations :

- **en 2015, le nombre d'incidents détectés a augmenté de 38 % par rapport à 2014;**
- **le coût total moyen d'une atteinte à la protection des données s'établissait à 4 millions de dollars américains chez les sociétés ayant participé au sondage.**

Dans l'Avis 2016, les ACVM présentent d'abord un récapitulatif de leurs récents projets pour surveiller les cyberrisques en vue d'une amélioration globale de la résilience dans nos marchés. Par exemple, après avoir constaté que de nombreux émetteurs ne communiquaient pas pleinement leur exposition aux cyberrisques, les ACVM ont indiqué dans l'Avis 2016 à leur personnel qu'elles comptent revoir l'information fournie par certains grands émetteurs dans les mois à venir et communiquer avec eux, le cas échéant, pour comprendre leur évaluation de l'importance des risques liés à la cybersécurité et aux cyberattaques. Les ACVM font également état de leurs projets actuels portant sur l'amélioration de l'échange d'information sur la cybersécurité entre organismes de réglementation internationaux.

L'Avis 2016 fournit aussi des liens et des références vers plusieurs ressources utiles en matière de cybersécurité, qui ont été publiées par divers organismes de réglementation et de normalisation pour améliorer la préparation aux cyberincidents des participants au marché, notamment les suivantes :

- ***Guide de pratiques exemplaires en matière de cybersécurité* de l'OCRCVM**[14]
- ***Gestion des cyberincidents – Guide de planification* de l'OCRCVM**[15]
- **Directives sur l'information à fournir de la Division of Corporation Finance de la Securities and Exchange Commission (SEC)**[16]
- **Cadre de cybersécurité du National Institute for Standards and Technology (NIST)**[17]
- **Conseils sur l'autoévaluation en matière de cybersécurité du Bureau du surintendant des institutions financières (BSIF)**[18]

Comme nous l'avons mentionné, la SEC a fourni des lignes directrices relatives à la divulgation des risques liés à la cybersécurité. L'information sur les facteurs de risque est propre à l'entité, mais dans le document « CF Disclosure Guidance: Topic No. 2 – Cybersecurity », la SEC indique que les facteurs de risque liés à la cybersécurité qui suivent devraient être divulgués, en fonction de leur importance et des faits et circonstances propres à l'émetteur : i) éléments de l'entreprise ou des activités de l'émetteur inscrit qui donnent lieu à des risques liés à la cybersécurité importants, et coûts et conséquences possibles, ii) dans la mesure où des activités présentant des risques importants liés à la cybersécurité sont imparties, une

14 En ligne à l'adresse http://www.ocrcvm.ca/industry/Documents/CybersecurityBestPracticesGuide_fr.pdf.

15 En ligne à l'adresse http://www.ocrcvm.ca/industry/Documents/CyberIncidentManagementPlanningGuide_fr.pdf.

16 En ligne à l'adresse https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

17 En ligne à l'adresse http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

18 En ligne à l'adresse http://www.osfi-bsif.gc.ca/fra/fi-if/in-ai/pages/cbrsk.aspx.

description de ces activités et de la façon dont les risques sont gérés par l'émetteur, iii) une description des cyberincidents, importants individuellement ou dans leur ensemble, dont l'émetteur a été victime, ainsi qu'une description des coûts et des autres conséquences, iv) les risques liés aux cyberincidents qui pourraient ne pas avoir été détectés pendant longtemps et v) toute couverture d'assurance pertinente[19]. Dans ses lignes directrices, la SEC précise que l'information propre à l'entité devrait être divulguée, mais que les lois sur les valeurs mobilières n'obligent pas à divulguer de l'information qui compromettrait la sécurité de l'émetteur. L'objectif est plutôt de fournir aux investisseurs assez d'information pour qu'ils comprennent la nature des risques de l'émetteur, sans que la sécurité de ce dernier soit compromise.

De plus, il est possible que les émetteurs doivent divulguer les cyberincidents connus ou réels pour que les investisseurs disposent de suffisamment d'éléments contextuels, tels que les coûts et les autres conséquences, pour comprendre la nature des risques. Par ailleurs, si un cyberincident amène un changement important, un communiqué de presse doit être déposé et diffusé, puis une déclaration de changement important doit être déposée.

COUVERTURE D'ASSURANCE

L'organisation possède-t-elle une assurance contre les cyberrisques? Si c'est le cas, l'incident est-il couvert et dans quelle mesure? Pour le déterminer, il faut lire les contrats et les politiques. De plus, les contrats d'assurance exigent généralement que l'assuré avise rapidement l'assureur s'il soupçonne un incident. L'organisation doit connaître le moment où cette obligation s'applique, le délai dont elle dispose pour le signalement et les renseignements requis.

Une fois cette vérification effectuée, il faut aviser l'assureur, mais seulement après avoir consulté le conseiller juridique et obtenu son approbation.

INDEMNISATION ET (OU) RESPONSABILITÉ DES TIERS OU DES EMPLOYÉS

Si un tiers (comme un fournisseur de services de TI) est impliqué dans la perte de données, on doit relire les contrats pertinents pour voir s'ils contiennent des clauses d'indemnisation et pour connaître les obligations de signalement et de communication de l'information qui y sont prévues.

Une fois cette vérification effectuée, il faut aviser au besoin le fournisseur de services tiers, mais seulement après avoir consulté le conseiller juridique et obtenu son

19 « CF Disclosure Guidance: Topic No. 2 – Cybersecurity », Division of Corporation Finance, Securities and Exchange Commission, 13 octobre 2011, accessible en ligne à l'adresse http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

approbation.

Les obligations et (ou) la responsabilité des employés peuvent également entrer en ligne de compte. Un examen doit être réalisé pour déterminer si les politiques de l'entreprise ont été respectées ou si des lois ont été enfreintes. Les mesures appropriées doivent être prises. De plus, si l'organisation est syndiquée, il est possible qu'on doive tenir compte des normes du travail.

5. Forces de l'ordre

Les forces de l'ordre peuvent intervenir dans deux situations : lorsqu'elles demandent des renseignements à l'organisation ou lorsque celle-ci fait appel à elles pour leur demander d'intervenir.

L'organisation doit être au fait des restrictions en matière de divulgation, surtout en ce qui concerne les renseignements personnels. Si les forces de l'ordre s'adressent à elle, l'organisation ne peut leur transmettre de renseignements personnels sans le consentement des personnes touchées que si un mandat ou une sommation l'exige, ou si la loi l'autorise. La question de savoir si une organisation peut divulguer les renseignements personnels demandés par les forces de l'ordre si la loi ne l'oblige pas à le faire est complexe et évolue sans cesse en fonction de la jurisprudence établie par la Cour suprême.

Les forces de l'ordre peuvent aussi intervenir lorsque l'organisation a conclu qu'elle était victime d'une infraction criminelle (voir l'encadré).

Après leur intervention, les forces de l'ordre peuvent demander que les avis sur la brèche et autres communications soient retardés afin de préserver l'intégrité de leur enquête, ou encore interdire la communication de certains renseignements, ce qui peut entrer en conflit avec les obligations réglementaires et contractuelles de l'organisation. Pour cette raison, un conseiller juridique doit participer à toutes les discussions avec les forces de l'ordre.

INFRACTIONS AU CODE CRIMINEL

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

Le vol d'identité se définit comme la possession et le trafic de **renseignements identificateurs sur une autre personne** qui sont utilisés dans l'intention de commettre un acte criminel dont l'un des éléments constitutifs est énuméré (supercherie, fraude, etc.). La fraude à l'identité consiste **à se faire passer pour une autre personne** afin d'obtenir un avantage pour soi-même ou de causer un désavantage à la victime.

Utilisation non autorisée d'ordinateur (art. 342.1)

Quiconque accède frauduleusement à un ordinateur ou à un système de stockage de données **qui ne lui appartient pas** pour télécharger de l'information ou intercepter des communications privées (un ancien employé mécontent qui pirate un système informatique de l'organisation, par exemple) commet une infraction.

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

Ce paragraphe criminalise **l'utilisation non autorisée de données qui rend ces dernières moins utiles pour leur propriétaire.** Veuillez noter qu'il ne s'applique pas au vol de renseignements confidentiels, et qu'il est difficile de placer ce dernier sous le régime d'une autre infraction au *Code criminel* existante, car la Cour suprême du Canada a jugé que les renseignements confidentiels ne constituent pas

Interception d'une communication privée (art. 184)

Il est illégal d'intercepter une communication privée ou d'y accéder lorsque les personnes concernées ont une **attente raisonnable en matière de vie privée.**

Terrorisme (art. 83.01-83.21)

Ces articles peuvent s'appliquer au **piratage de grande envergure** qui vise à mettre en danger la vie et à compromettre la sécurité de la population, ou à perturber un service essentiel, dans un but de nature politique, religieuse ou idéologique. Quiconque participe à une telle activité de piratage, la facilite ou donne des instructions à cet égard commet une infraction.

6. Protection des consommateurs/clients

L'une des parties prenantes les plus importantes en cas d'atteinte à la protection des données est la clientèle de l'organisation. Les attentes des consommateurs canadiens sont élevées : en plus de vouloir être avisés rapidement de tout incident, ils souhaitent que l'organisation prenne immédiatement des mesures claires pour les protéger (ou leur permettre d'agir pour se protéger eux-mêmes). L'écart entre les actions de l'organisation et les attentes des consommateurs est source de risque.

Entre autres, l'organisation doit envisager la création d'un centre d'appel pour répondre aux questions des consommateurs. De plus, ceux-ci s'attendent souvent à ce qu'une organisation victime d'un incident important, qui touche des cartes de crédit ou des renseignements personnels, offre une surveillance du crédit et (ou) une protection contre le vol d'identité.

Une réponse réfléchie et robuste aux questions de la clientèle peut non seulement contribuer à conserver les clients et à préserver la valeur de la marque, mais aussi avoir une incidence notable sur les risques d'actions collectives et les dommages-intérêts et honoraires connexes[20].

CENTRES D'APPEL

En cas d'atteinte à la protection des données de très grande envergure, on prendra la décision de mettre en place un centre d'appel (plutôt que de confier les demandes des clients à des ressources internes, afin qu'elles soient traitées au cas par cas). Plus vite le centre d'appel est fonctionnel, plus vite l'organisation peut commencer à contrôler le message et à limiter le risque d'atteinte à la réputation et de litige.

20 Voir, par exemple, l'affaire *Lozanski v The Home Depot, Inc.*, 2016 ONSC 5447 (CanLII), à l'adresse http://canlii.ca/t/gt65j, où le juge Perell a observé que le plan d'intervention d'un défendeur peut bien être un facteur décisif de l'abandon ou du règlement d'une action collective : « Les arguments à l'appui de la culpabilité de Home Depot étaient dès le départ de nature spéculative et se sont au bout du compte révélés très faibles… Après la découverte de l'atteinte à la vie privée, il n'y a pas eu de camouflage, et Home Depot a agi en entreprise socialement responsable pour remédier à la situation. Il n'y a pas lieu de croire qu'elle devait ou méritait de changer de comportement. L'indemnisation que Home Depot a volontairement accordée à ses clients est supérieure à celle des actions collectives… Au moment du règlement des actions collectives contre Home Depot, les pertes réelles des membres du groupe n'avaient pu être démontrées et les représentants des demandeurs n'étaient même pas membres du groupe visé par le règlement. On ne saurait prétendre le contraire : Home Depot est la partie gagnante, car elle a su résister à une réclamation de 500 millions de dollars.» (parag. 100-101) [traduction libre]

CENTRES D'APPEL – POINTS À CONSIDÉRER	
☐	Le fournisseur de services peut-il garantir à l'organisation un numéro sans frais unique pour ses clients?
☐	Le numéro sera-t-il vraiment sans frais, et fonctionnera-t-il dans tous les territoires concernés?
☐	Le fournisseur de services peut-il offrir ce service en tout temps?
☐	Pendant combien de temps l'organisation prévoit-elle avoir besoin du centre d'appel? Si elle ne le sait pas encore, la période d'activité peut-elle être de durée indéterminée?
☐	Le processus d'inscription aux services de protection est-il simple et facile à comprendre? L'organisation doit réfléchir à la façon dont elle déterminera qui est admissible à ces services; dans la plupart des cas, les critères des entreprises sont faibles ou inexistants, ce qui évite d'accroître le mécontentement des clients.
☐	Le fournisseur de services offre-t-il des modèles de script et de foires aux questions personnalisables par l'organisation?
☐	Le fournisseur de services parle-t-il couramment le français et l'anglais? D'autres langues?
☐	Tous les documents doivent être revus par les services juridiques pour que le message et le langage soient uniformes. Dans quels délais les services juridiques peuvent-ils revoir et approuver les scripts et les foires aux questions?
☐	Le processus d'inscription des clients aux services de protection du fournisseur de services est-il simple?
☐	L'organisation aura-t-elle le dernier mot sur tous les scripts ou le fournisseur de services utilisera-t-il ses propres formulations, voire profitera-t-il de l'occasion pour approcher les clients?
☐	Peut-on s'adresser à un expert des fraudes, s'il y a lieu?
☐	Le fournisseur peut-il offrir des services de suivi et de production de rapports? L'organisation aura besoin de renseignements pour suivre les progrès des efforts de résolution de l'incident. Des éléments comme le nombre d'appels traités par jour, le type d'appels et le délai de réponse doivent être considérés.

SERVICES DE PROTECTION

Habituellement, deux grands types de services de protection sont offerts : les services de protection du crédit et les services de **protection contre le vol d'identité**. La protection du crédit comprend le suivi du crédit des clients sans frais et l'envoi d'alertes aux clients dont le rapport de crédit présente des activités ou des éléments nouveaux. La protection contre le vol d'identité comprend le suivi du permis de conduire, du numéro d'assurance sociale et d'autres pièces d'identité importantes ainsi que des activités en ligne dans le but de vérifier si des renseignements personnels y sont achetés ou vendus, et le suivi des archives judiciaires et d'autres sources pouvant indiquer une possibilité de fraude à l'identité.

Ces services de protection pourraient ne pas être requis dans tous les cas. Une organisation victime d'un incident doit choisir avec soin les services qu'elle offrira et savoir, si elle décide de ne pas offrir certains d'entre eux, que sa décision sera étudiée de près, surtout s'il apparaît plus tard qu'une telle protection aurait été justifiée. L'offre de services de ce type contribue également à l'atténuation des dommages possibles, ce qui sera pris en considération dans tout litige subséquent.

Soulignons que les services de protection offerts aux États-Unis diffèrent beaucoup de ceux qu'on retrouve au Canada. Si un incident touche les deux territoires, les entreprises doivent s'attendre à ce qu'on leur demande pourquoi les services offerts dans un territoire sont meilleurs, sont en vigueur plus longtemps ou sont plus complets que dans l'autre. Les questions peuvent être moins nombreuses si les déclarations publiques ne décrivent pas la nature des services fournis, mais indiquent simplement qu'ils sont offerts.

DÉDOMMAGEMENT

Dans certains cas, les services de protection contre la fraude ou le vol d'identité peuvent ne pas être appropriés ni réalisables. Il arrive aussi que la confiance des consommateurs soit en jeu. L'organisation peut alors envisager un dédommagement. Idéalement, cette question aura été étudiée bien avant qu'un incident survienne, et l'organisation aura déterminé clairement la forme de ce dédommagement, sa répartition, son montant, etc. (par exemple, une carte-cadeau de 10 $ à tous les clients qui présentent la preuve d'un achat effectué au cours d'une certaine période).

ABOUT McCARTHY TÉTRAULT'S CYBERSECURITY, PRIVACY AND DATA MANAGEMENT GROUP

Data incidents at major retailers, government departments and financial services organizations should serve as a clear warning to all organizations doing business in Canada that collect, use and/or disclose personal information. Consumers actively expect that these entities should take market-leading steps to protect personal and financial data.

Increasingly, good information management practices go beyond matters of privacy. Malicious hacks (from outside and from within) and ransomware demands have targeted intellectual property, trade secrets and other critical business information with noticeable impacts on share prices, director and Board longevity, and industry competitiveness. Clients need support from counsel who can marry legislative compliance and the application of industry codes of conduct and privacy policies in various jurisdictions with a practical knowledge of commercial and technology outcomes - all in a manner that will help a client preserve privilege.

Cybersecurity, protection of business information and data, and strategic management of the production and/or retention of information are all significant aspects of our practice. Our privacy and data management lawyers offer perspective on all aspects of information management, storage and transfer. Mitigating risk for clients is always our first priority and we have helped clients manage the entire lifecycle of data, including providing guidance to companies looking to prepare for and prevent a critical data incident. When crisis occurs, we draw from a team of leading class action litigators and subject matter specialists who have responded to some of the highest profile data incidents in North America and are involved in many of the key cybersecurity initiatives (both private and public) in Canada.

For more information please contact:

À PROPOS DU GROUPE CYBERSÉCURITÉ, CONFIDENTIALITÉ ET GESTION DES DONNÉES DE MCCARTHY TÉTRAULT

Des atteintes à la protection des données d'importants détaillants, ministères et établissements de services financiers devraient servir d'avertissement clair à toutes les organisations en activité au Canada qui collectent, utilisent ou divulguent des renseignements personnels sur les particuliers. Les consommateurs s'attendent à ce que ces entités prennent des mesures de pointe en vue de protéger les renseignements personnels et financiers.

Les bonnes pratiques de gestion de l'information débordent de plus en plus du cadre de la confidentialité. Les attaques malveillantes (externes ou internes) et les demandes de rançongiciels visent la propriété intellectuelle, les secrets commerciaux et d'autres renseignements d'affaires sensibles ayant des répercussions notoires sur le prix des actions, la longévité d'un directeur et d'un conseil d'administration, ainsi que sur la compétitivité dans l'industrie. Les clients ont besoin du soutien d'avocats capables d'assurer à la fois le respect de la loi et l'application des codes de déontologie de l'industrie ainsi que des politiques de confidentialité des diverses entités, et la mise à profit d'une connaissance pratique des résultats commerciaux et technologiques – tout en les aidant à préserver le secret professionnel.

La cybersécurité, la protection des renseignements et des données d'affaires, ainsi que la gestion stratégique de la production ou la rétention de l'information constituent des aspects importants de notre activité. Nos avocats spécialisés en confidentialité et en gestion des données offrent une perspective sur tous les aspects de la gestion, du stockage et du transfert de l'information. Nous cherchons toujours, en priorité, à limiter les risques pour nos clients. Nous les aidons à gérer l'ensemble du cycle de vie des données et conseillons les entreprises qui souhaitent se préparer à contrer et à prévenir toute atteinte importante à la protection de leurs données. En cas d'urgence, nous disposons d'une équipe d'éminents avocats plaidants en matière d'actions collectives et d'experts en la matière qui sont intervenus dans le cadre de certaines des atteintes à la protection des données les plus notoires en Amérique du Nord, et dont les membres participent à bon nombre d'initiatives clés en matière de cybersécurité (à la fois privées et publiques) au Canada.

Pour obtenir plus d'information, veuillez communiquer avec :

TORONTO

Dan Glover
416-601-8069
dglover@mccarthy.ca

Christine Ing
416-601-7713
christineing@mccarthy.ca

Barry Sookman
416-601-7949
bsookman@mccarthy.ca

MONTRÉAL

Charles Morgan
514-397-4230
cmorgan@mccarthy.ca

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.

Version 3 – révisée en janvier 2017