CGI

La force de l'engagement[MD]

La législation canadienne en matière de cybersécurité aura-t-elle des répercussions sur votre entreprise?

Soyez conscient de vos obligations.

En 2015, le gouvernement du Canada a introduit plusieurs modifications législatives et programmes gouvernementaux afin de suivre l'évolution de l'économie numérique et de parer aux cybermenaces croissantes à l'endroit des entreprises et des citoyens du Canada. Ces initiatives, qui ont pour but de renforcer notre cyberrésilience collective, exigent que toutes les entreprises canadiennes, quelle que soit leur taille, et toutes les organisations canadiennes qui hébergent des données personnelles, mettent à jour leurs feuilles de route en matière de cybersécurité pour s'assurer d'exercer leurs activités en toute conformité. La présente étude offre un sommaire de ces initiatives afin d'aider les clients de CGI à s'adapter aux nouvelles exigences et à assurer la protection des renseignements de leurs clients.

Contexte

En 2010, la Stratégie de cybersécurité du Canada établissait un programme stratégique afin de s'attaquer aux cybermenaces croissantes. En 2015, le gouvernement est passé à l'action avec un plan prévoyant une nouvelle législation et un financement accru pour la mise en œuvre de cette stratégie. Le secteur privé sera directement touché par ces initiatives. Le gouvernement rappelle aux chefs de la direction et aux conseils d'administration qu'ils ont l'obligation de protéger les renseignements personnels de leurs clients et employés, et que leurs entreprises sont exposées à des risques s'ils ne prennent pas les mesures adéquates pour protéger cette information.

La Stratégie de cybersécurité du Canada comportait trois objectifs :

1. protéger les systèmes gouvernementaux,
2. nouer des partenariats pour protéger les cybersystèmes essentiels à l'extérieur du gouvernement fédéral, et
3. aider les Canadiens à se protéger en ligne. Il n'y a rien d'étonnant à ce que l'objectif principal de la stratégie ait d'abord consisté à accroître la résilience des propres systèmes du gouvernement.[1]

Mais au cours des dernières années, le gouvernement a pris des mesures pour transposer ces objectifs en actions qui comprenaient des éléments de soutien du secteur privé.[2] Les documents consultatifs suivants ont notamment été préparés:

- *Guide Pensez cybersécurité pour les petites et moyennes entreprises*[3] – Document « pour aider les Canadiens qui possèdent ou gèrent une petite ou une moyenne entreprise à comprendre les risques auxquels ils sont confrontés en matière de cybersécurité; le guide leur fournit des conseils pratiques sur la façon de mieux protéger leur entreprise et ses employés contre la cybercriminalité. »
- *Sécurité informatique et systèmes de contrôle industriel (SCI) Pratiques exemplaires recommandées*[4] – Rapport technique « destiné aux professionnels et gestionnaires des TI des gouvernements fédéral, provinciaux et territoriaux, des administrations municipales, des infrastructures critiques et des autres industries qui exploitent ou gèrent des systèmes de surveillance et d'acquisition de données (SCADA) ou des systèmes de commande de processus (SCI). »
- *Cadre de gestion des incidents cybernétiques pour le Canada*,[5] – Approche collaborative qui « attribue les rôles et les responsabilités de tous les ordres de gouvernement, de tous les propriétaires et exploitants d'infrastructures essentielles ainsi que d'autres partenaires des secteurs public et privé dans une intervention coordonnée en matière de prévention, d'atténuation, de préparation, d'intervention et de rétablissement par suite d'incidents qui touchent la portion canadienne du cyberespace. »

> « L'annonce qui a été faite aujourd'hui visant l'adoption de nouvelles mesures pour protéger les systèmes cybernétiques essentiels est encourageante. »
>
> L'honorable Sergio Marchi, président-directeur général de l'Association canadienne de l'électricité

[1] « Stratégie de cybersécurité du Canada Renforcer le Canada et accroître sa prospérité », 2010 : http://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-fra.pdf

[2] « Plan d'action 2010-2015 de la Stratégie de cybersécurité du Canada », 2013 : http://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-fr.aspx

[3] « Guide Pensez cybersécurité pour les petites et moyennes entreprises » : http://www.pensezcybersecurite.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-fr.aspx

[4] « Sécurité informatique et systèmes de contrôle industriel (SCI) Pratiques exemplaires recommandées » 10 décembre 2012 : http://www.securitepublique.gc.ca/cnt/rsrcs/cybr-ctr/2012/tr12-002-fr.aspxx

[5] « Cadre de gestion des incidents cybernétiques pour le Canada », août 2013 : http://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/cbr-ncdnt-frmwrk/index-fr.aspx

Changements ayant des répercussions sur les affaires

Parmi les nombreux changements présentés en 2015, les chefs d'entreprise se souviendront qu'en janvier, certaines sections de la Loi canadienne anti-pourriel sont entrées en vigueur en ce qui a trait à l'installation non sollicitée de programmes informatiques ou de logiciels.[6] Le gouvernement a également entrepris trois autres initiatives en matière de cybersécurité en 2015.

1. Dispositions de la Loi sur la protection des renseignements personnels numériques concernant la déclaration obligatoire des atteintes à la sécurité
2. Législation prévue en vertu de laquelle les exploitants des cybersystèmes essentiels seront tenus de mettre en œuvre des plans de cybersécurité et de signaler les incidents liés à la cybersécurité au gouvernement du Canada
3. Financement accru afin d'accroître la capacité du gouvernement à aider le secteur privé à se protéger contre les cyberattaques

> « Manley a déclaré que le secteur privé saluait la coopération du gouvernement fédéral dont les organismes peuvent enquêter sur les cyberattaques et poursuivre en justice les auteurs de cybercrimes. »

Les paragraphes suivants présentent de plus amples renseignements sur chacune de ces initiatives, de même que des mesures recommandées pour les entreprises.

Déclaration obligatoire des atteintes à la sécurité

En 2015, la Loi sur la protection des renseignements personnels numériques a créé de nouvelles obligations légales pour les compagnies subissant une atteinte à la sécurité des renseignements personnels. Ces organisations sont maintenant tenues de prendre les mesures suivantes.

- Déclarer au commissaire toute atteinte aux mesures de sécurité concernant les 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 »[7]
- Aviser les personnes concernées si leurs renseignements ont été perdus ou volés, et si elles courent un risque de préjudice important – il peut s'agir, par exemple, d'un vol d'identité ou de tout effet négatif sur leur dossier de crédit[8]
- Veiller à ce que l'avis soit effectué « le plus tôt possible après que l'organisation a conclu qu'il y a eu atteinte »[9]
- Conserver et tenir à jour un registre de ces atteintes à la sécurité.[10]

La loi a pour objectif d'encourager les entreprises à protéger adéquatement les renseignements personnels et à assurer à leurs clients que leurs renseignements personnels sont en sécurité. Les non-conformités pourraient être coûteuses, avec des amendes allant jusqu'à 100 000 $ si l'organisation omet d'aviser le commissaire ou ne tient pas à jour un registre de chaque atteinte aux mesures de sécurité ayant trait aux renseignements personnels. En réalité, l'atteinte à la réputation des entreprises pourrait être encore plus coûteuse.

Mesure recommandée – Le Cabinet n'a pas encore proclamé la mise en force de ces dispositions relatives à la déclaration des atteintes à la sécurité en vertu de la Loi sur la protection des renseignements personnels numériques; on ne sait donc pas encore comment elles seront appliquées. Cependant, le secteur privé doit dès maintenant commencer à penser aux mesures à prendre pour se conformer à ce nouveau régime juridique. Les systèmes d'information et de gestion des événements relatifs à la sécurité pourront avoir une importance accrue en tant qu'outils aidant les compagnies à respecter leurs nouvelles obligations.

> « Le secteur privé subit des attaques régulières et constantes sur ses cybersystèmes. Ces attaques ne surviennent pas seulement chaque semaine ou chaque mois, mais bien chaque jour et de façon répétée. »
>
> L'honorable John Manley, président et chef de la direction du Conseil canadien des chefs d'entreprise et coprésident du Comité consultatif des chefs de la direction sur la cybersécurité

[6] Faits en bref – Loi canadienne anti-pourriel, gouvernement du Canada, http://fightspam.gc.ca/eic/site/030.nsf/fra/h_00039.html

[7] Projet de loi S-4, Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques et une autre loi en conséquence, S.10.1(1)

[8] Section 10.1(3) et 10.1(7)

[9] Section 10.1(6)

[10] Section 10.3(1)

Législation entourant les cybersystèmes essentiels

Il importe de souligner, pour le secteur privé, que l'intention du gouvernement d'alors était d'introduire une nouvelle loi par laquelle « les exploitants des cybersystèmes essentiels seront tenus, en vertu de nouvelles lois, de mettre en œuvre des plans de cybersécurité, d'obtenir de solides résultats en ce qui a trait à la sécurité de leurs systèmes et de signaler les incidents liés à la cybersécurité au gouvernement du Canada ».[11] Les consultations débuteront dès la publication de l'avant-projet de loi.

Mesure recommandée – Les entreprises croyant qu'elles ne constituent pas un exploitant de cybersystèmes essentiels et ne se croyant donc pas concernées par la législation proposée pourraient devoir réexaminer leur position. La Stratégie nationale et le Plan d'action sur les infrastructures essentielles énumèrent les dix secteurs qui sont considérés comme essentiels par le gouvernement. Ce sont la santé, les finances, les communications et technologies de l'information, l'énergie et les services publics, l'alimentation, l'eau, le secteur manufacturier, le transport, la sécurité et le gouvernement. Bien que les cybersystèmes essentiels n'aient pas encore été définis, il est probable qu'il s'agira d'un sous-ensemble de ces dix secteurs. Il faudra déterminer si une compagnie n'étant pas directement visée par la définition sera quand même affectée en tant que maillon de la chaîne d'approvisionnement en biens ou services fournis à un cybersystème essentiel.

Augmentation du financement du gouvernement pour les initiatives de cybersécurité

En 2015, plusieurs initiatives du gouvernement ont eu pour but de mieux protéger, grâce à une collaboration accrue entre les secteurs public et privé, les cybersystèmes essentiels à l'extérieur du gouvernement fédéral, et de prendre des mesures à l'encontre des cybercriminels. Ces initiatives ont été applaudies par le secteur privé.

Le budget fédéral et le Plan d'action économique de 2015 contenaient deux annonces liées à la cybersécurité qui auront un impact sur le secteur privé. Le financement approuvé par le Parlement, qui se poursuivra jusqu'à ce qu'il soit amendé par le nouveau gouvernement, comprend:

- 58 millions de dollars en nouveau financement pour les cinq prochaines années afin de mieux protéger les cybersystèmes et l'infrastructure essentiels du Canada contre les cyberattaques;
- 36,4 millions de dollars en nouveau financement sur cinq ans pour soutenir les efforts du gouvernement en vue de sécuriser les cybersystèmes essentiels du Canada. Le financement ne sera pas directement accordé au secteur privé mais sera plutôt utilisé pour « soutenir davantage les exploitants grâce à l'élaboration et à la diffusion d'outils de cybersécurité, de renseignements sur la sécurité et d'une expertise pour mettre en œuvre de nouvelles lois. »[12]

[11] « Plan d'action économique », ministre des Finances, 21 avril 2015, **http://www.budget.gc.ca/2015/docs/plan/budget2015-fra.pdf**

[12] « Plan d'action économique », ministre des Finances, 21 avril 2015, chapitre 4.3, **http://www.budget.gc.ca/2015/docs/plan/budget2015-fra.pdf**

En juillet 2015, le ministre de la Sécurité publique et de la Protection civile annonçait du financement additionnel pour les initiatives de cybersécurité afin d'aider le secteur privé à composer avec les cyberattaques : 142,6 millions de dollars ont été ajoutés au financement annoncé dans le budget.

Ce financement sera dirigé vers trois initiatives :

1. Centre canadien de réponse aux incidents cybernétiques (CCRIC)[13]
   Le CCIRC verra un accroissement « important » de sa capacité à répondre aux incidents dans le secteur privé et grâce à « l'élaboration d'alimentations automatisées en temps réel »[14], le secteur privé recevra des renseignements supplémentaires sur les menaces et la diffusion sera accélérée.[15]
2. Programme d'évaluation de la résilience régionale (PERR)
   Ce programme comprend « [...] un projet d'évaluation de sites effectué en coopération avec les États-Unis afin de renforcer la résilience des infrastructures essentielles des deux pays » et inclut la participation des propriétaires et exploitants des installations du secteur privé. « Ce financement renforcera la capacité du PERR à intégrer la cybersécurité dans le processus d'évaluation de sites. Grâce à cette mesure, Sécurité publique Canada pourra évaluer la cybersécurité générale d'une organisation et formuler des recommandations en vue de la rendre plus résiliente. »[16]
3. Application de la loi
   La Gendarmerie royale du Canada (GRC) améliorera sa capacité de détection de la cybercriminalité de haut niveau et de lutte contre celle-ci grâce à une équipe spéciale d'enquêteurs, une capacité accrue du renseignement, un soutien technique et une formation sur l'application de la loi.

Conclusion

Ces initiatives du gouvernement signalent aux entreprises l'importance d'un cyberenvironnement sécurisé afin de protéger les renseignements personnels et de l'entreprise. Le financement accru pour les programmes gouvernementaux destinés à venir en aide au secteur privé, conjugué avec les nouveaux régimes juridiques ayant trait aux cybersystèmes essentiels et aux atteintes à la sécurité des renseignements personnels, méritent une attention particulière de la part des chefs d'entreprises. Les nouvelles mesures de financement du gouvernement contribueront à retenir leur attention.

Les chefs d'entreprise peuvent s'attendre à d'autres interventions du gouvernement en matière de cybersécurité. La lettre de mandat du ministre de la Sécurité publique et de la Protection civile de décembre 2015 détermine que les « grandes priorités » du ministre doivent inclure la direction d'un « examen des mesures en place pour assurer la protection des Canadiens et des infrastructures critiques du Canada contre les cybermenaces… »[17]

Les solutions de CGI

Puisque les experts en cybersécurité de CGI travaillent autant avec les secteurs civils et de la défense au gouvernement qu'avec le secteur privé, nous demeurons bien informés de ces nouvelles réalités et des changements dans les exigences législatives. Nous nous adaptons continuellement pour aider nos clients à s'assurer que leurs feuilles de route en matière de sécurité et leurs politiques et procédures de collecte de renseignements sont à jour et harmonisées avec la nouvelle réglementation de notre pays.

[13] « Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) fonctionne au sein de Sécurité publique Canada, et il vise à sécuriser les systèmes cybernétiques des provinces, des territoires, des municipalités et des organisations du secteur privé. Le CCIRC offre divers documents d'orientation et conseils techniques aux professionnels de la sécurité pour les aider à assurer la sécurité de leurs entreprises. » **http://www.pensezcybersecurite.gc.ca/cnt/prtct-yrslf/prtct-smlbsn/index-fr.aspx**

[14] Gouvernement du Canada, Sécurité publique Canada, Document d'information, « Faire progresser la Stratégie de cybersécurité du Canada » et CBC News, 22 juillet 2015, « Steven Blaney announces new funding for cyber security » par Susana Mass

[15] Gouvernement du Canada, Sécurité publique Canada, Document d'information, « Faire progresser la Stratégie de cybersécurité du Canada » et ITWorld Canada, 22 juillet 2015, « Ottawa increases spending to protect critical infrastructure from cyber attacks », par Howard Solomon

[16] Idem

[17] Lettre de mandat du ministre de la Sécurité publique et de la Protection civile: **http://pm.gc.ca/fra/lettre-de-mandat-du-ministre-de-la-securite-publique-et-de-la-protection-civile**

CGI

cgi.com

Fondée en 1976, CGI est l'une des plus importantes entreprises de services en technologies de l'information (TI) et en gestion des processus d'affaires au monde et offre des services-conseils en management ainsi que des services d'intégration de systèmes et de gestion déléguée de grande qualité. Grâce à son solide engagement à offrir des solutions et services novateurs, CGI affiche un bilan inégalé de 95 % de projets réalisés selon les échéances et budgets prévus. Nos équipes s'arriment aux stratégies d'affaires des clients afin d'obtenir des résultats probants sur toute la ligne.