OSLER

Le projet de loi C-8 du Canada : ce que les entreprises doivent savoir au sujet du nouveau cadre de cybersécurité

19 JUIN 2026 25 MIN DE LECTURE

Expertises Connexes

- Cybersécurité et intervention en cas d'incident lié à la sécurité
- Défense, sécurité et aérospatiale
- Énergie nucléaire
- Pipelines
- Respect de la vie privée et gestion de l'information
- Services bancaires et financiers
- Technologie
- Télécom

Auteurs(trice): Éloïse Gratton, Ad. E., Adam LaRoche, Tina Saban, Naomi Chernos

Introduction

Le projet de loi C-8, *Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois*, établit le cadre de cybersécurité le plus important jamais adopté au Canada par le gouvernement fédéral. Le projet de loi crée un double régime : il élargit les pouvoirs du gouvernement fédéral pour sécuriser le système de télécommunications du Canada et établit pour les exploitants de cybersystèmes essentiels dans les secteurs sous réglementation fédérale des obligations de cybersécurité susceptibles d'exécution forcée.

Le projet de loi C-8 succède au projet de loi C-26, qui avait été présenté lors de la législature précédente, mais n'avait pas été adopté avant la prorogation du Parlement. Il a été présenté à nouveau l'année dernière sous une forme sensiblement similaire à celle du projet de loi C-8 lors de la 45e législature. Le projet de loi a franchi une étape importante le 16 juin 2026, lorsqu'il a reçu la sanction royale. Ayant désormais achevé son parcours parlementaire, ses dispositions de fond entreront en vigueur à une date ou à des dates à fixer par décret du gouverneur en conseil, de nombreux détails opérationnels devant être précisés ultérieurement par voie de règlement. En revanche, les modifications à la *Loi sur les télécommunications* prévues à la Partie 1 (décrites plus en détail ci-dessous) sont désormais en vigueur.

Le texte législatif répond à un ensemble de menaces en constante évolution – fréquence croissante des incidents, mouvements latéraux à travers les réseaux et ciblage des fournisseurs de services – et rapproche l'approche du Canada de celles de ses principaux alliés, notamment les États-Unis (*Cyber Incident Reporting for Critical Infrastructure Act of 2022* (la CIRCIA)), l'Union européenne (la directive SRI 2) et le Royaume-Uni (*Network and Information Systems Regulations 2018* (le règlement SRI)). Dans le présent bulletin d'actualités, nous présentons un résumé des principales dispositions, leurs implications sur la protection des renseignements personnels et les activités commerciales, ainsi que les mesures concrètes que les organisations devraient envisager de prendre.

Aperçu et structure

Le projet de loi C-8 comprend deux parties fonctionnelles :

- **Partie 1 — Modifications apportées à la *Loi sur les télécommunications* :** Cette partie ajoute la promotion de la sécurité du système canadien de télécommunications aux objectifs de la politique en la matière et confère au gouverneur en conseil et au ministre de l'Industrie des pouvoirs étendus leur permettant d'ordonner aux fournisseurs de services de télécommunications (FST) de prendre, ou de s'abstenir de prendre, des mesures particulières afin de sécuriser le système.
- **Partie 2 — *Loi sur la protection des cybersystèmes essentiels* (LPCE) :** Cette partie édicte une nouvelle loi établissant des obligations de cybersécurité détaillées pour les « exploitants désignés » de « cybersystèmes essentiels » dans les secteurs sous réglementation fédérale, ainsi que des mécanismes de vérification, d'ordres de conformité et de sanctions.

La partie 3 prévoit l'examen par le Parlement des dispositions édictées et modifiées par la Loi dans les cinq ans suivant sa sanction. Ensemble, les deux parties fonctionnelles établissent un régime à plusieurs niveaux comprenant des obligations, des pouvoirs d'édiction de directives gouvernementales et des outils d'application de la loi qui auront une incidence significative sur la manière dont les entreprises exploitant des infrastructures essentielles gèrent les cyberrisques.

Partie 1 : Modifications apportées à la *Loi sur les télécommunications*

La partie 1 confère des pouvoirs importants au gouverneur en conseil et au ministre de l'Industrie leur permettant de prendre, selon le cas, des décrets ou des arrêtés portant sur la sécurité à l'intention des FST. L'article 15.1 confère au gouverneur en conseil le pouvoir de prendre des décrets interdisant aux FST d'utiliser les produits ou les services d'une personne déterminée ou leur ordonnant de les retirer de leurs réseaux ou installations. L'article 15.2 confère au ministre une longue liste de pouvoirs, notamment le pouvoir de prendre des arrêtés interdisant aux FST d'utiliser des produits ou des services déterminés, leur imposant des conditions quant à leur utilisation, exigeant qu'ils mettent fin à des ententes de service, exigeant qu'ils élaborent des plans de sécurité, que soient menées des évaluations de vulnérabilité et que soient mises en œuvre des normes, et, en vertu d'une disposition générale prévue à l'alinéa 15.2(2)m), leur ordonnant de faire ou de s'abstenir de faire toute chose déterminée.

Ces pouvoirs fournissent une base légale formelle aux décisions d'exclusion de fournisseurs du type de celles que le Canada a déjà prises concernant les équipements 5G et élargissent considérablement la capacité du gouvernement à intervenir de manière continue dans les décisions des FST en matière d'approvisionnement, de gestion des fournisseurs et de sécurité des réseaux. L'étendue des pouvoirs conférés par les articles 15.1 et 15.2 constitue donc l'un des aspects les plus importants de la Loi.

L'exercice de ces pouvoirs est soumis à un certain nombre de caractéristiques et de protections clés.

Caractéristiques et protections clés

- **Nécessité et proportionnalité :** La portée et la teneur des dispositions d'un décret ou d'un arrêté doivent être nécessaires et raisonnables eu égard à la gravité de la menace. Avant de prendre un décret ou un arrêté, le décideur doit tenir compte de l'effet de la prise du décret ou de l'arrêté sur les activités des FST, ses répercussions financières, son effet sur la fourniture de services de télécommunications et ses répercussions sur la protection de la vie privée.
- **Décrets ou arrêtés confidentiels :** Un décret ou un arrêté peut comprendre une disposition interdisant à toute personne de divulguer l'existence de celui-ci ou de son contenu, sous réserve d'une liste de facteurs dont le décideur doit tenir compte, notamment l'effet de la non-divulgation sur les principes de transparence et de responsabilisation. Le décideur doit aviser le Comité des parlementaires sur la sécurité nationale et le renseignement et l'Office de surveillance des activités en matière de sécurité nationale et de renseignement de la prise de tout décret ou arrêté secret.
- **Limites strictes :** Le ministre ne peut ordonner aux FST d'intercepter une communication privée ou une communication radiotéléphonique ni ordonner le décryptage d'une communication privée chiffrée, au sens de l'article 183 du *Code criminel*.
- **Aucune indemnisation; primauté des décrets et des arrêtés :** Il convient de noter qu'aucune indemnisation n'est due pour les pertes financières résultant d'un décret ou d'un arrêté, et que les dispositions des décrets et des arrêtés l'emportent sur les dispositions incompatibles de toute décision prise par le CRTC. La *Loi sur les textes réglementaires* ne s'applique ni aux décrets ni aux arrêtés.

Application de la loi

Toute contravention à une disposition d'un décret, d'un arrêté ou d'un règlement pris en vertu des articles 15.1 ou 15.2 constitue une violation exposant son auteur à une pénalité dont le montant maximal est, **dans le cas d'une personne physique, de 25 000 $** (**50 000 $** en cas de récidive) et, **dans les autres cas, de 10 millions de dollars** (**15 millions de dollars** en cas de récidive). En outre, quiconque contrevient à un tel décret, à un tel arrêté ou à un tel règlement commet une infraction passible, sur déclaration de culpabilité par procédure sommaire, d'une amende que le tribunal estime indiquée et, s'il s'agit d'une personne physique, d'un emprisonnement maximal de deux ans moins un jour.

Un contrôle judiciaire est possible, mais selon des règles spéciales : le ministre peut retirer des éléments de preuve de la procédure, et le juge désigné de la Cour fédérale ne doit pas fonder sa décision sur les éléments retirés et doit en préserver la confidentialité. Il convient de noter que la Loi n'établit **pas** de régime d'avocat spécial, et les modifications qui prévoyaient l'obligation d'obtenir l'autorisation d'un tribunal avant la prise de tout décret ou arrêté ont été jugées irrecevables lors de l'examen en Chambre. Le régime tel qu'il a été adopté repose donc sur le pouvoir discrétionnaire de l'exécutif, lequel fait l'objet d'un contrôle a posteriori au moyen d'examens, de rapports annuels au Parlement et d'avis aux organismes chargés de la surveillance de la sécurité nationale. Cette structure a suscité des critiques en matière d'équité procédurale et au regard de la *Charte*, en particulier des préoccupations selon lesquelles les parties concernées pourraient ne pas être en mesure de connaître ou de contester le fondement des décrets ou des arrêtés, et que, à défaut d'avocat spécial, il n'y a plus de partie indépendante apte à examiner les preuves du gouvernement

dans le cadre de procédures à huis clos.

Partie 2 : La *Loi sur la protection des cybersystèmes essentiels*

La partie 2 constitue le cœur du projet de loi. La LPCE établit des obligations de cybersécurité susceptibles d'exécution forcée pour les entités considérées comme des « exploitants désignés » de « cybersystèmes essentiels » et répartit la surveillance entre six organismes réglementaires sectoriels.

Personnes concernées

La LPCE s'applique aux « exploitants désignés », c.-à-d. à toute personne, société de personnes ou organisation non dotée de la personnalité morale qui appartient à une catégorie d'exploitants figurant à l'annexe 2. Bien que l'annexe 2 soit actuellement vierge, il s'agira de catégories d'exploitants qui possèdent ou exploitent un « cybersystème essentiel », soit tout cybersystème dont la compromission, en ce qui touche la confidentialité, l'intégrité ou la disponibilité, pourrait menacer la continuité ou la sécurité d'un service critique ou d'un système critique. L'annexe 1 énumère six catégories de services critiques et de systèmes critiques :

- services de télécommunications
- systèmes de pipelines et de lignes électriques interprovinciaux ou internationaux
- systèmes d'énergie nucléaire
- systèmes de transport relevant de la compétence législative du Parlement
- systèmes bancaires
- systèmes de compensations et de règlements.

Le gouverneur en conseil peut ajouter à l'annexe 1 un service ou un système sous réglementation fédérale s'il est convaincu que le service ou le système est critique pour la sécurité nationale ou la sécurité publique; il peut également ajouter de nouvelles catégories d'exploitants et désigner un organisme réglementaire pour chacune d'entre elles, de sorte que le champ d'application pourrait s'étendre au fil du temps. La surveillance est répartie entre le surintendant des institutions financières, la Banque du Canada, les ministres de l'Industrie et des Transports, la Régie canadienne de l'énergie et la Commission canadienne de sûreté nucléaire, chacun disposant de pouvoirs d'inspection, de vérification interne et d'émission d'ordres de conformité à l'égard des catégories qui lui sont attribuées.

Il importe de préciser que les obligations prévues par la LPCE ne s'appliquent qu'aux « cybersystèmes essentiels » de l'exploitant, c'est-à-dire les systèmes dont la compromission, en ce qui touche la confidentialité, l'intégrité ou la disponibilité, pourrait menacer la continuité ou la sécurité d'un service critique ou d'un système critique. Même si tous les exploitants seront, en vertu de leur désignation, considérés comme responsables de cybersystèmes essentiels, les processus des exploitants qui ne peuvent pas être considérés comme ayant une incidence sur un système critique ou un service critique ne seront pas soumis aux exigences de la LPCE. Puisqu'une telle définition va au-delà de la technologie exploitée dans le cadre de leurs activités, les exploitants devront déterminer de manière justifiable quels sont les systèmes qui seraient considérés comme soumis à ces exigences, en fonction de leur implication et de leur incidence sur les catégories de systèmes critiques et de services critiques (qui sont généralement considérés comme relevant des « infrastructures essentielles »), et quelles exigences de la LPCE s'appliqueraient.

Principales obligations

- **Programmes de cybersécurité (article 9) :** Dans les 90 jours suivant la date à laquelle il devient membre d'une catégorie déterminée, l'exploitant est tenu d'établir un programme de cybersécurité permettant : a) d'identifier et de gérer les cyberrisques, notamment les risques associés à la chaîne d'approvisionnement et aux tiers, b) de protéger ses cybersystèmes essentiels contre toute compromission, c) de détecter les incidents de cybersécurité, d) de réduire au minimum les conséquences des incidents et e) de prendre toute autre mesure prévue par règlement. L'exploitant doit fournir le programme à l'organisme réglementaire compétent dans le délai susmentionné, doit le mettre en œuvre et en assurer la mise à jour, et doit en entreprendre l'examen au moins une fois par an.
- **Risques associés à la chaîne d'approvisionnement et aux tiers (article 15) :** En plus de gérer les risques associés à la chaîne d'approvisionnement et aux tiers conformément à l'obligation générale prévue à l'article 9, l'exploitant est tenu d'atténuer ces risques *dès* qu'ils ont été identifiés, notamment par la prise de mesures conformes aux lignes directrices élaborées par le Centre de la sécurité des télécommunications (CST). Il s'agit de l'une des exigences les plus exigeantes sur le plan opérationnel. Cela impose un niveau de gestion des risques associés aux fournisseurs que de nombreuses organisations n'ont pas encore formalisé. Compte tenu du fait que de nombreux contrats sont en cours, les organisations devraient désormais veiller à ce que leurs engagements respectent les cadres et normes internationalement reconnus en matière d'atténuation des risques de cybersécurité dans les relations avec les fournisseurs, et prévoir des droits de recours appropriés.
- **Signalement des incidents (paragraphes 17-18) :** Il incombe à tout exploitant désigné de déclarer, dans les délais réglementaires, lesquels ne doivent pas dépasser 72 heures, tout incident de cybersécurité concernant l'un de ses cybersystèmes essentiels au CST. Le seuil est large : un incident à signaler est un incident qui nuit *ou peut nuire* soit à la continuité ou à la sécurité d'un service critique ou d'un système critique, soit à la confidentialité, à l'intégrité ou à la disponibilité du cybersystème essentiel. Par ailleurs, sans délai après avoir déclaré l'incident au CST, l'exploitant doit en aviser l'organisme réglementaire compétent et lui remettre une copie du rapport d'incident. La Loi maintient expressément la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), de sorte que les obligations de déclaration prévues par la LPCE s'appliquent parallèlement aux obligations existantes en matière d'avis en cas d'atteinte à la vie privée.
- **Directives de cybersécurité (article 20) :** Le gouverneur en conseil peut, par décret, donner des directives enjoignant à un exploitant désigné, individuellement ou au titre de son appartenance à une catégorie, de se conformer aux mesures prévues en vue de la protection d'un cybersystème essentiel. La portée et la teneur des dispositions de la directive doivent être raisonnables, et le gouverneur en conseil doit tenir compte des répercussions du décret sur les activités opérationnelles, la sécurité publique, la protection de la vie privée, les finances et la fourniture des services. Il est interdit à tout exploitant désigné visé par une directive d'en communiquer l'existence ou le contenu, sauf dans la

mesure nécessaire pour s'y conformer (articles 24 et 25), et les mêmes limites en matière de chiffrement et d'interception qui s'appliquent à la partie 1 s'appliquent ici.

- **Tenue de documents (article 30) :** Les exploitants doivent tenir des documents concernant la mise en œuvre du programme, les incidents déclarés, les mesures d'atténuation des risques associés à la chaîne d'approvisionnement, les mesures prises pour mettre en œuvre toute directive de cybersécurité, ainsi que toute autre question précisée par règlement, et doivent conserver ces documents au Canada. Ils peuvent également faire l'objet de vérifications et de contrôles de conformité par leur organisme réglementaire.

Sanctions et application

- Le montant de la **sanction pécuniaire administrative** applicable à chaque violation est plafonné, **dans le cas d'une personne physique, à 500 000 $ et, dans les autres cas, à 15 millions de dollars**, et il est compté une violation distincte pour chacun des jours au cours desquels se continue une violation. Il s'agit là des plafonds prévus par la loi; le montant de la sanction applicable à une violation particulière et la classification des violations seront fixés par règlement.
- **Infractions :** Certaines contraventions – notamment le fait de ne pas établir ou mettre en œuvre un programme, de ne pas atténuer les risques associés à la chaîne d'approvisionnement et de violer la confidentialité d'une directive – constituent des infractions passibles de sanctions et, s'il s'agit d'une personne physique, d'un emprisonnement maximal de deux ans moins un jour sur déclaration de culpabilité par procédure sommaire ou de cinq ans sur déclaration de culpabilité par mise en accusation.
- **Responsabilité personnelle :** En cas de perpétration d'une violation ou d'une infraction par une organisation, les administrateurs et les dirigeants qui l'ont ordonnée ou autorisée, ou qui y ont consenti, acquiescé ou participé, sont considérés comme des coauteurs de la violation ou de l'infraction, que l'organisation fasse ou non l'objet d'une procédure en violation ou d'une poursuite.
- **Disculpation :** La prise des précautions voulues peut être invoquée relativement à toute violation et à la plupart des infractions, ce qui traduit l'importance de documenter les efforts de conformité et de les communiquer au conseil d'administration. En outre, la Loi n'a pas pour effet de porter atteinte au secret professionnel de l'avocat.

L'ampleur de ces sanctions et la possibilité d'invoquer la prise des précautions voulues soulignent que la conformité se doit d'être une priorité de gouvernance au niveau du conseil d'administration.

Implications pour les lois sur la protection des renseignements personnels

Le projet de loi C-8 se situe clairement à la croisée des lois sur la cybersécurité et sur la protection des renseignements personnels. En matière de protection des renseignements personnels, les équipes juridiques doivent anticiper les problèmes suivants.

Transmission de renseignements au gouvernement

Les deux parties contiennent des dispositions générales sur l'échange de renseignements permettant le partage de renseignements – y compris de renseignements confidentiels – entre des organismes fédéraux tels que le CST, le Service canadien du renseignement de sécurité (SCRS), le ministère de la Défense nationale et les organismes réglementaires sectoriels à des fins liées aux décrets, aux arrêtés et aux règlements.

La Loi prévoit plusieurs mesures aux fins de la protection des renseignements personnels, y compris l'obligation de retirer les renseignements personnels lorsqu'ils ne sont plus nécessaires, des restrictions sur la collecte, l'utilisation et la communication de renseignements personnels et de renseignements dépersonnalisés au-delà de ce qui est raisonnable par rapport à la menace visée, ainsi que des dispositions portant qu'« il est entendu » que les dispositions de la *Loi sur la protection des renseignements personnels* et de la LPRPDE continuent de s'appliquer.

Malgré ces mesures de protection, le Commissariat à la protection de la vie privée et des groupes de défense des libertés civiles ont exprimé des préoccupations au cours du processus législatif concernant l'étendue des pouvoirs de partage de renseignements, le volume de renseignements pouvant être transmis aux institutions gouvernementales à l'insu des personnes concernées, ainsi que l'adéquation des mécanismes de surveillance. En conséquence, dans la pratique, l'efficacité des mesures de protection des renseignements personnels prévues par la Loi dépendra vraisemblablement de manière significative du contenu des règlements à venir et de la manière dont le régime sera effectivement mis en œuvre.

Conséquences pour les organisations

Compte tenu du chevauchement et de l'incidence du projet de loi C-8 sur des domaines traditionnellement régis par les lois existantes en matière de protection des renseignements personnels, les organisations devraient réfléchir à la manière de gérer les obligations qui se chevauchent en matière de protection des renseignements personnelsCompte tenu du chevauchement et de l'incidence du projet de loi C-8 sur des domaines traditionnellement régis par les lois existantes en matière de protection des renseignements personnels, les organisations devraient réfléchir à la manière de gérer les obligations qui se chevauchent en matière de protection des renseignements personnels.

Par exemple, les obligations de déclaration des incidents prévues par la LPCE (au CST) chevauchent les obligations de déclaration des atteintes à la vie privée prévues par la LPRPDE. Le régime d'avis en cas d'atteinte de la LPRPDE exige qu'une déclaration soit faite au Commissaire à la protection de la vie privée « le plus tôt possible » (ce qui signifie généralement quelques jours) et que les personnes intéressées soient avisées s'il existe un « risque réel de préjudice grave ». En revanche, la LPCE impose un délai strict de 72 heures (la durée exacte devant être fixée par règlement), un seuil plus bas (les incidents qui « peuvent nuire » à un service critique ou à un système critique) et un destinataire différent (le CST, avec copie immédiate à l'organisme réglementaire sectoriel). Comme la Loi laisse expressément la LPRPDE intacte, les organisations devront mettre en place des processus coordonnés de réponse aux incidents qui satisfont aux deux régimes selon les délais et les seuils qui leur sont propres, en plus de l'ensemble de plus en plus complexe d'obligations d'avis en cas d'atteinte qui s'appliquent aux organisations exerçant leurs activités dans des secteurs réglementés, telles que celles imposées aux institutions financières sous réglementation fédérale par le Bureau du surintendant des institutions financières (BSIF) ou celles applicables aux entités réglementées en vertu de la *Loi sur la sûreté et la réglementation nucléaires* du Canada. Les organisations assujetties à la *Loi sur la protection des*

renseignements personnels dans le secteur privé du Québec (récemment modifiée par la Loi 25) devront faire face à une couche supplémentaire d'exigences provinciales en matière d'avis, assorties de leurs propres délais.

De plus, les dispositions autorisant les décrets ou arrêtés confidentiels et les directives de non-divulgation peuvent limiter la manière et la rapidité avec lesquelles les organisations peuvent communiquer leurs décisions en matière de sécurité aux personnes concernées et aux autres parties prenantes. Une telle limitation pourrait se répercuter sur l'intensité des efforts requis pour aviser les intéressés en cas d'incident.

Implications en droit commercial, considérations pratiques et mesures à prendre

Chaîne d'approvisionnement et marchés publics

Les organisations devront revoir les contrats qu'elles ont conclus avec des tiers et, dans de nombreux cas, les renégocier afin d'y ajouter des exigences en matière de cybersécurité, des droits de vérification, des dispositions concernant les avis en cas d'incident et des déclarations de conformité. Comme l'obligation d'atténuer les risques associés à la chaîne d'approvisionnement dès que ceux-ci ont été identifiés est expressément stipulée à l'article 15, une telle obligation constitue une exigence réglementaire et non une simple bonne pratique. Dans le but de s'acquitter d'une telle obligation permanente, les organisations devraient commencer dès maintenant à revoir et à renforcer leurs méthodes de gestion des risques associés à la chaîne d'approvisionnement, notamment en mettant à jour les contrats qu'elles ont conclus avec des tiers, y compris les dispositions concernant la cybersécurité, les droits de vérification et les avis en cas d'incident.

Restrictions imposées aux fournisseurs et actifs immobilisés

Le pouvoir du gouvernement d'interdire ou d'imposer le retrait de produits de fournisseurs déterminés crée de l'incertitude sur le plan commercial et un risque associé à des actifs immobilisés, les deux étant aggravés par le fait que la Loi ne prévoit aucun droit à indemnisation. Les organisations devraient élaborer des protocoles internes pour la réception et le traitement des décrets, des arrêtés et des directives confidentiels du gouvernement, y compris les contraintes de non-divulgation qui y sont associées.

Gouvernance d'entreprise et désignation

En raison à la fois de l'ampleur des sanctions potentielles, du risque de responsabilité des administrateurs et des dirigeants, ainsi que de l'obligation d'établir un programme officiel, il est absolument nécessaire que le conseil d'administration exerce une cybergouvernance et reçoive à intervalles réguliers des rapports sur les risques et l'état de conformité. Dans un premier temps, les organisations doivent déterminer si elles sont susceptibles d'être des exploitants désignés, en se basant sur les secteurs énumérés à l'annexe 1 et sur leur profil réglementaire, et identifier quels sont leurs systèmes susceptibles d'être considérés comme des cybersystèmes essentiels. Elles devraient ensuite procéder à une analyse des lacunes de leur programme de cybersécurité actuel par rapport aux cinq éléments prévus par la Loi, en sachant que le délai de 90 jours commence à courir dès la publication du décret établissant les exploitants désignés. Elles devraient aussi mettre en place au niveau de leur conseil d'administration des mécanismes de cybergouvernance et de déclaration démontrant leur conformité et étayant la prise des précautions voulues.

Assurance

Le cadre pourrait avoir une incidence sur la souscription et la couverture des cyberassurances. Les organisations devraient revoir leur couverture de cyberassurance à la lumière des nouveaux risques liés aux sanctions et aux mesures correctives, et vérifier si les sanctions réglementaires, les coûts de mise en conformité et les mesures correctives imposées par le gouvernement sont couverts.

Fusions et acquisitions, et investissements

Le statut d'entité se conformant à la loi deviendra un élément important des vérifications diligentes dans le cadre des opérations visant des exploitants désignés – y compris les mesures d'application de la loi en cours et le coût des mesures correctives – et pourrait être compliqué par les décrets, les arrêtés ou les directives confidentiels qu'une cible ne pourrait pas divulguer intégralement. Les organisations se livrant à des activités de fusion et d'acquisition et d'investissement devraient intégrer la conformité au projet de loi C-8 dans leurs programmes de vérification diligente dans le cas des opérations visant des exploitants susceptibles d'être considérés comme des exploitants désignés.

Considérations transfrontalières

Les exploitants exerçant des activités au pays et à l'étranger doivent concilier le projet de loi C-8 avec les régimes qui le chevauchent, notamment la CIRCIA des États-Unis, la directive SRI 2 de l'UE et le règlement SRI du Royaume-Uni.

Intervention en cas d'incident et coordination avec les lois sur la protection des renseignements personnels

Les organisations devraient instaurer des mécanismes de détection des incidents et d'intervention en cas d'incident les assurant de remettre les avis en cas d'incident, dans le cas de l'avis à remettre au CST, dans le délai de 72 heures prévu par la Loi et, dans le cas de l'avis à remettre aux organismes réglementaires, de façon immédiate, le tout de façon coordonnée avec les obligations d'avis en cas d'atteinte prévues par la LPRPDE. Elles devraient également évaluer l'interaction entre les nouvelles obligations de cybersécurité et les programmes existants de conformité aux lois sur la protection des renseignements personnels, y compris les principes de minimisation des collectes de données et de limitation des fins pour lesquelles les données sont collectées.

Surveillance des règlements d'application

Les organisations devraient surveiller activement les règlements d'application, car ceux-ci définiront les exploitants désignés, les seuils et délais de déclaration, les exigences des programmes et le montant des sanctions. En s'engageant sans tarder auprès des organismes réglementaires sectoriels et des groupes industriels, les organisations seront mieux à même d'anticiper les exigences particulières qui s'appliqueront à leur cas, et de s'y préparer.

Conclusion

Le projet de loi C-8 marque un tournant dans la réglementation canadienne en matière de cybersécurité. Pour la première fois, les exploitants d'infrastructures essentielles sous réglementation fédérale seront soumis à des obligations de cybersécurité détaillées susceptibles d'exécution forcée, assorties de pénalités financières et de sanctions pénales considérables. Bien que de nombreux détails restent à préciser par voie de règlements, la direction à suivre est claire, et les fondements de la conformité – un programme solide, des méthodes renforcées de gestion des risques associés à la chaîne d'approvisionnement, des mécanismes de détection et de signalement efficaces, ainsi qu'une gouvernance au niveau du conseil d'administration – nécessitent des investissements soutenus qui ne peuvent être mis en place du jour au lendemain. Les organisations des secteurs concernés devraient commencer à se préparer dès maintenant.

Bien que le cadre législatif soit désormais largement défini, d'importantes incertitudes opérationnelles subsistent. De nombreux détails seront précisés par voie de règlements, notamment les entités qui seront désignées, les seuils particuliers de signalement des incidents dans le délai maximal de 72 heures et les éléments devant figurer dans les programmes de cybersécurité. Des questions subsistent également concernant la portée pratique des pouvoirs de prendre des décrets ou des arrêtés confidentiels, l'adéquation du processus de contrôle judiciaire modifié, l'interaction du régime avec les futures réformes des lois fédérales sur la protection des renseignements personnels dans le secteur privé, et la question de savoir si les petits exploitants des secteurs désignés bénéficieront finalement d'exemptions fondées sur l'importance relative ou la taille.

Osler continuera de suivre l'évolution du projet de loi C-8 et l'élaboration des règlements d'application, et publiera d'autres bulletins d'actualités à mesure que la situation évoluera.