Le projet de loi C-8 relance la réforme canadienne en cybersécurité — Ce que doivent savoir les secteurs d'infrastructures critiques

28 juillet 2025

Faits saillants

Que s'est-il passé?

Le gouvernement Carney a relancé un cadre réglementaire étendu en matière de cybersécurité avec le projet de loi C-8, qui vise à renforcer les exigences de conformité pour les secteurs d'infrastructures critiques de compétence fédérale, notamment les services bancaires, les transports, l'énergie et les télécommunications.

Pourquoi est-ce important?

Les obligations en matière de cybersécurité imposées aux exploitants désignés qui assurent des services ou systèmes critiques sont à la fois rigoureuses et étendues. Une fois la loi adoptée, les organisations devront mettre en place des programmes de cybersécurité exhaustifs, signaler tout changement important à leurs systèmes (notamment ceux entraînant des répercussions sur la sécurité nationale), et déclarer immédiatement tout incident de cybersécurité. Les violations pourraient entraîner des amendes allant jusqu'à 15 M$ *par jour* pour les organisations.

Que pouvez-vous faire?

Les organisations d'infrastructures critiques devraient prendre des mesures proactives et faire appel à des ressources externes pour se préparer à respecter les obligations en matière de cybersécurité prévues par le projet de loi, qui devrait être adopté rapidement à la reprise des travaux parlementaires à l'automne. Ces mesures incluent : cartographier les systèmes critiques; comprendre les nouveaux pouvoirs des organismes réglementaires compétents; élaborer et mettre en œuvre les plans et les formations nécessaires pour renforcer la cyberrésilience; et se doter de la capacité de réagir efficacement aux incidents et aux enquêtes qui peuvent s'ensuivre, afin de limiter les risques et la responsabilité.

Le 18 juin 2025, 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, a été déposé à la Chambre des communes afin de combler les lacunes dans la capacité du gouvernement fédéral à protéger les systèmes d'infrastructures critiques. Ce projet de loi relance notamment les vastes obligations en matière de cybersécurité et les pouvoirs réglementaires qui avaient été proposés initialement dans le cadre du projet de loi C-26 (déposé trois ans plus tôt, mais jamais adopté).

Bien que largement identique au projet de loi C-26 (sur lequel BLG avait publié un article en juin 2022), le projet de loi C-8 introduit plusieurs changements importants. Parmi ceux-ci figurent la révision des procédures de contrôle judiciaire ainsi que le retrait des modifications conséquentes à la *Loi sur la preuve au Canada* (qui visaient à protéger les renseignements sensibles déposés dans le cadre de contrôles judiciaires ou d'appels).

Même si le projet de loi C-8 doit suivre l'ensemble du processus législatif, ses similitudes avec C-26, combinées au fait que ce dernier avait presque été adopté avant la prorogation du Parlement, laissent croire qu'il pourrait progresser rapidement. Les organisations relevant de secteurs fédéraux, notamment les services bancaires, les transports, l'énergie et les télécommunications, devraient dès maintenant se préparer à ces changements majeurs.

Obligations de conformité

La Loi sur la protection des cybersystèmes essentiels (LPCE) proposée dans le cadre du projet de loi C-8 impose des obligations rigoureuses en matière de cybersécurité aux exploitants désignés de cybersystèmes critiques fédéraux. Ces exploitants assurent des services ou des systèmes critiques, c'est-à-dire des infrastructures essentielles à la sécurité nationale et à la sécurité publique.

Ces obligations comprennent notamment :

- Établir, mettre en œuvre et réviser régulièrement les programmes de cybersécurité;
- Aviser l'organisme réglementaire compétent de tout changement important dans la propriété, le contrôle ou l'utilisation de produits et services de tiers, afin d'atténuer les risques liés à la chaîne d'approvisionnement et aux tiers;
- Respecter les directives de cybersécurité émises par le gouverneur en conseil;
- Déclarer les incidents de cybersécurité au Centre de la sécurité des télécommunications dans un délai de 72 heures;
- Conserver des documents détaillés sur les programmes et incidents de cybersécurité.

Malheureusement, la LPCE offre peu d'orientations concrètes, les exigences énoncées étant formulées de manière générale. Les obligations précises – notamment celles liées à l'établissement, à la mise en œuvre et au maintien des programmes de cybersécurité – seront définies ultérieurement par règlement. Les exploitants désignés doivent donc,

dès à présent, dresser un inventaire complet de leurs cybersystèmes et en évaluer la criticité.

Ce manque de détails législatifs est aggravé par le pouvoir du gouvernement d'émettre des directives contraignantes (et confidentielles) en matière de cybersécurité. De plus, aucune obligation ne prévoit la consultation des exploitants désignés avant l'émission de telles directives. Par exemple, une directive pourrait exiger la mise en œuvre de mesures de sécurité précises, sans consultation préalable quant à leur faisabilité opérationnelle, leurs implications financières ou leurs effets sur la continuité des services.

Supervision et application sectorielles

Un aspect central du projet de loi C-8 est la délégation de vastes pouvoirs sectoriels à l'organisme de réglementation compétent :

- **Systèmes bancaires :** supervision assurée par le Bureau du surintendant des institutions financières (BSIF).
- **Systèmes de compensations et de règlements :** supervision assurée par la Banque du Canada.
- **Systèmes de pipelines et de lignes électriques interprovinciaux ou internationaux :** supervision assurée par la Régie de l'énergie du Canada.
- **Systèmes d'énergie nucléaire :** supervision assurée par la Commission canadienne de sûreté nucléaire.
- **Services de télécommunications :** supervision assurée par le ministre de l'Industrie.
- **Systèmes de transport relevant de la compétence législative du Parlement :** supervision assurée par le ministre des Transports.

Plus précisément, le projet de loi C-8 autorisera ces organismes de réglementation à :

- Pénétrer dans tout lieu (y compris une propriété privée, à l'exception toutefois d'une maison d'habitation sans consentement ou sans mandat) et examiner tout ce qui s'y trouve, y compris les registres, rapports ou données;
- Ordonner des vérifications internes des pratiques, des livres et d'autres documents;
- Émettre des ordres de conformité contraignants exigeant que les exploitants désignés cessent toute activité non conforme ou prennent des mesures correctives dans un délai déterminé;
- Recueillir ou communiquer des renseignements, y compris des renseignements confidentiels, pourvu que le ministre ou le ministre compétent soit convaincu que les renseignements considérés comme confidentiels seront traités comme tels.

Le projet de loi C-8 réintroduit par ailleurs des sanctions administratives pécuniaires (SAP) importantes en cas de violation. Bien que le régime proposé vise à favoriser la conformité, les amendes pourraient atteindre 15 M$ par violation, *par jour*, pour une organisation – et 1 M$ par violation, *par jour*, pour une personne physique. De plus, les dirigeants et administrateurs des exploitants désignés pourraient être tenus personnellement responsables s'ils ont participé à la commission d'une violation.

Les violations peuvent être contestées, notamment en invoquant la prise des précautions voulues. Un accord de conformité peut également être conclu avec l'organisme de réglementation compétent. Une telle transaction peut prévoir une réduction partielle ou totale du montant de la pénalité, mais vaut déclaration de responsabilité à l'égard de la violation. En cas de défaut d'exécution, la pénalité complète deviendrait exigible et la violation pourrait être rendue publique.

Votre organisation est-elle prête?

Les exploitants désignés devraient prendre des mesures proactives pour mettre en place des programmes et des pratiques de cybersécurité robustes, en vue de répondre aux obligations attendues du projet de loi C-8. Pour réduire leur exposition aux sanctions potentielles et renforcer leur état de préparation à l'échelle de leurs opérations, les organisations responsables d'infrastructures critiques devraient :

- Évaluer si votre organisation est un exploitant désigné au sens de la LPCE et obtenir du soutien externe pour cartographier l'ensemble des systèmes, services et opérations pouvant être considérés comme critiques;
- Déterminer quel organisme de réglementation assure votre conformité à la LPCE et envisager des échanges préalables sur les implications du projet de loi pour votre secteur;
- Mettre en place des cadres de gouvernance avec des voies de responsabilité claires, en désignant les personnes et équipes responsables de développer et de mettre en œuvre les procédures requises pour satisfaire aux obligations de conformité;
- Renforcer votre capacité interne à réagir tant aux incidents de cybersécurité qu'aux inspections, audits et ordres de conformité qui pourraient suivre – notamment au moyen d'exercices de simulation et de mises en situation réelles;
- Réévaluer de façon continue vos obligations en fonction de l'évolution des menaces et des mises à jour réglementaires.

Être préparé ne signifie pas seulement que votre organisation sera prête pour l'adoption probable du projet de loi C-8. Cela vous permettra, à vous et à votre équipe, de bénéficier d'un avantage stratégique pour faire face à l'évolution constante du paysage des cybermenaces.

Communiquez avec nous

Le groupe Cybersécurité, respect de la vie privée et protection des renseignements personnels de BLG, ainsi que nos avocats spécialisés en IA, suivent de près l'évolution rapide des lois en matière de cybersécurité et de vie privée. Ils peuvent vous aider à comprendre les obligations qui incombent à votre organisation et à vous préparer efficacement à l'entrée en vigueur du projet de loi C-8.

N'hésitez pas à contacter les personnes-ressources ci-dessous pour toute question concernant le projet de loi C-8 et ses répercussions possibles sur votre organisation.

Par

Hélène Deschamps Marquis, Matt Saunders, Chloe Hughes-Légaré, Aaron Grech

Services

Cybersécurité, respect de la vie privée et protection des renseignements personnels, Technologies de l'information, Gouvernance, Services bancaires et financiers, Technologies, Intelligence artificielle (IA), Transports, Énergie – Pétrole et gaz, Énergie – Électricité

BLG | Vos avocats au Canada

Borden Ladner Gervais S.E.N.C.R.L., S.R.L. (BLG) est le plus grand cabinet d'avocats canadien véritablement multiservices. À ce titre, il offre des conseils juridiques pratiques à des clients d'ici et d'ailleurs dans plus de domaines et de secteurs que tout autre cabinet canadien. Comptant plus de 725 avocats, agents de propriété intellectuelle et autres professionnels, BLG répond aux besoins juridiques d'entreprises et d'institutions au pays comme à l'étranger pour ce qui touche les fusions et acquisitions, les marchés financiers, les différends et le financement ou encore l'enregistrement de brevets et de marques de commerce.

blg.com

Bureaux BLG

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000, rue De La Gauchetière Ouest
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749