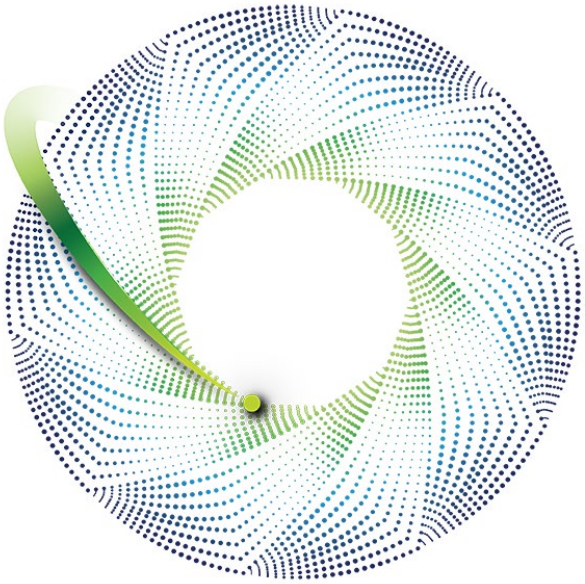
Deloitte.



Alerte canadienne – Fiscalité et Services juridiques

Cybermenaces dans le secteur de l’énergie et au-delà

Pourquoi et comment votre organisation devrait aborder les vulnérabilités en matière de cybersécurité

Le 3 novembre 2021

Sommaire

Les cybercriminels ciblent des sources de données plus diversifiées et il y a eu une flambée de la prévalence et du pouvoir destructeur des cyberattaques dans le secteur de l’énergie à travers le monde au cours des dernières années. Cet article examine les risques juridiques spécifiques auxquels font face tant les organisations que les administrateurs et dirigeants, et présente un certain nombre de recommandations pour atténuer cette responsabilité.

Considérations importantes

L'environnement actuel de la cybersécurité dans le secteur de l'énergie

La portée et l'importance des attaques par rançongiciels dans ce secteur ont augmenté. Prenons, par exemple, le récent incident impliquant Colonial Pipeline Co. qui a forcé la société à verser une rançon de près de 5 millions de dollars américains en monnaie numérique et, dans l'intervalle, à fermer près de 9 000 km d'oléoduc, provoquant ainsi des achats en panique dans les stations-service de l'Est des États-Unis. En outre, cet incident a mis en évidence à quel point certaines organisations publiques et privées, y compris celles du secteur de l'énergie, sont vulnérables aux attaques aussi élémentaires soient-elles visant les réseaux informatiques.

Bien que plusieurs aient spéculé sur les raisons sous-jacentes à la prévalence croissante de telles attaques, nos recherches ainsi que nos propres observations dans le cadre de notre travail avec des entreprises de services publics sur des incidents d'atteintes à la sécurité des données similaires nous ont permis d'identifier les éléments suivants :

1. **Une augmentation du nombre de menaces ainsi que des auteurs de menace ciblant les entreprises de services publics**

Une évaluation récente effectuée par le Centre canadien pour la cybersécurité a souligné que les **cybercriminels** ne sont pas les seuls à lancer des attaques dans le secteur de l'énergie afin d'obtenir le paiement de rançons, les fruits de fraudes commerciales et la propriété intellectuelle. Les **auteurs de cybermenace parrainés par des États** cherchent également à atteindre leurs objectifs géopolitiques et les « **hacktivistes** » cherchent à faire connaître leurs programmes et/ou leur opposition aux projets de certains services publics.

Beaucoup de ces auteurs de menace sont considérés par les services de renseignements gouvernementaux comme hautement sophistiqués et motivés à cibler la chaîne d'approvisionnement et les fournisseurs de services gérés pour deux raisons : (i) pour obtenir la propriété intellectuelle et des informations sur les systèmes de contrôle industriels (SCI) d'un service public; et (ii) comme accès par voie détournée aux réseaux de services publics d'électricité.

Le Centre canadien pour la cybersécurité note que « la probabilité qu'une cyberattaque puisse avoir un impact sur le secteur canadien de l'électricité est **plus élevée** qu'elle aurait pu l'être autrement en raison des **liens qui existent entre les réseaux électriques américains et canadiens**. Les auteurs de cybermenace considèrent probablement le Canada comme une cible intermédiaire par laquelle ils peuvent passer pour nuire au secteur américain de l'électricité. De plus, l'augmentation de l'activité de cybermenace visant les réseaux américains pourrait entraîner un événement susceptible de mettre en danger le secteur canadien de l'électricité. »

2. **La vulnérabilité particulière des entreprises d'électricité et de gaz aux cyberattaques**

Au cours des deux dernières années, les attaques par rançongiciels susceptibles d'affecter les processus industriels sont devenues plus fréquentes au Canada et dans le

Personnes-ressources :

Hélène Deschamps Marquis
Leader nationale de la pratique confidentialité des données et cybersécurité
Associée, Deloitte Legal Canada
Tél. : 514-393-8300

Claire Feltrin
Avocate principale,
Confidentialité des données et cybersécurité
Deloitte Legal Canada
Tél. : 416-885-9446

Liens connexes :

Services de fiscalité de Deloitte

Deloitte Legal Canada S.E.N.C.R.L./s.r.l.

monde entier. Depuis janvier 2019, par exemple, au moins sept variantes de rançongiciel contenaient des instructions pour mettre fin aux processus SCI qui s'exécuteraient normalement sur des postes de contrôle industriels[1].

L'une des causes possibles de cette augmentation pourrait être l'expansion constante de la surface d'attaque des services publics découlant de leur complexité géographique et organisationnelle. La nature essentiellement décentralisée du leadership en matière de cybersécurité de ces organisations et les interdépendances uniques du secteur de l'énergie électrique entre les infrastructures physiques et informatiques contribuent également à la vulnérabilité particulière de ces entreprises aux cyberattaques. Enfin, comme l'a souligné le Centre canadien pour la cybersécurité, les auteurs de cybermenace adaptent leurs activités aux nouvelles occasions que présente la transition des entreprises du secteur de l'énergie à la technologie du réseau intelligent.

Les exemples de telles attaques vont de l'appropriation des systèmes de technologie opérationnelle (TO) par les cybercriminels au moyen d'Internet, en passant par la fraude à la facturation au moyen des compteurs intelligents sans fil jusqu'à la destruction physique.

Les répercussions sur les organisations et les dirigeants/administrateurs

1. Les organisations

En vertu de la législation fédérale actuelle sur la protection des renseignements personnels dans le secteur privé (la *Loi sur la protection des renseignements personnels et les documents électroniques* ou LPRPDE), les organisations doivent :

- déclarer au commissaire à la protection de la vie privée du Canada les atteintes aux mesures de sécurité concernant des renseignements personnels présentant un risque réel de préjudice grave à des individus;
- aviser les intéressés au sujet de ces atteintes;
- conserver un registre de toutes les atteintes.

Toute organisation qui contrevient sciemment aux obligations aux termes de la LPRPDE en matière de déclaration, d'avis et de tenue de registre des atteintes aux mesures de sécurité se rend coupable d'une infraction, et pourrait se voir infliger des amendes. De plus, les modifications proposées à cette loi dans le projet de loi C-11, la *Loi sur la mise en œuvre de la Charte du numérique* (LMCN), visent à introduire (i) des sanctions administratives pécuniaires pour les organisations qui contreviennent à la nouvelle législation, jusqu'à concurrence de 10 000 000 $ et de 3 % du revenu global brut de l'organisation; et (ii) des amendes pouvant atteindre 25 000 000 $ et 5 % du revenu global brut de l'organisation lorsque les organisations contreviennent *sciemment* à certaines obligations que leur impose le nouveau régime.

Les organisations du secteur de l'énergie devraient également connaître la North American Electric Reliability Corporation (NERC), qui a élaboré des normes relatives aux

[1] Andy Greenberg, « Mysterious New Ransomware Targets Industrial Control Systems », *Wired*, 3 février 2020; Nathan Brubaker *et al.*, « Financially Motivated Actors Are Expanding Access Into OT: Analysis of Kill Lists That Include OT Processes Used With Seven Malware Families », blogue *FireEye Threat Research*, 15 juillet 2020.

incidents de cybersécurité et exige que les incidents de sécurité soient signalés à la NERC dans les délais prescrits selon l'incident en cause (en plus des rapports présentés au Commissariat à la protection de la vie privée du Canada en vertu de la LPRPDE)[2]. L'omission de déclarer de tels incidents peut entraîner des amendes et d'autres sanctions. En outre, les organisations assujetties à la Transportation Security Administration des États-Unis doivent respecter des exigences strictes relatives à la mise en œuvre de mises à jour et de correctifs de logiciels de cybersécurité dans le contexte d'incidents de sécurité[3].

Au-delà de ces amendes et sanctions prévues dans la loi et de la menace pour la sécurité nationale inhérente aux cyberattaques dans le secteur de l'énergie, les entreprises du secteur de l'énergie ciblées par des incidents de cybersécurité sont confrontées à d'autres risques uniques, notamment une interruption importante des activités des infrastructures critiques résultant d'attaques par déni de service distribué (DDoS pour *Distributed Denial of Service*), un risque d'atteinte à la réputation découlant de la méfiance des consommateurs après l'incident et d'éventuels recours collectifs.

2. Les dirigeants et les administrateurs

Bien que la responsabilité personnelle potentielle des dirigeants et des administrateurs en cas de défaillance de la cybersécurité demeure un domaine du droit canadien en cours d'élaboration, il est clair que ces personnes seraient bien avisées de jouer un rôle délibéré dans la gestion des risques de cybersécurité afin de s'acquitter de leurs obligations envers l'entreprise.

Par exemple, les administrateurs et les dirigeants ont des obligations, tant en vertu de la législation que de la common law canadienne, de faire preuve de diligence raisonnable dans le cadre de l'exploitation de l'entreprise. Ainsi, ils doivent identifier de manière proactive les lacunes en matière de cybersécurité, traiter régulièrement les problèmes de cybersécurité lors des réunions du conseil d'administration et des réunions connexes, et s'assurer que les incidents de sécurité critiques sont traités en temps opportun et signalés aux personnes appropriées. De plus, en vertu des lois fédérales et provinciales canadiennes sur la protection de la vie privée, les administrateurs et les dirigeants peuvent être tenus responsables des sanctions réglementaires. Au Québec, par exemple, les administrateurs et les dirigeants qui autorisent un acte ou une omission de l'entreprise qui contrevient à la législation sur la protection de la vie privée peuvent être désignés comme parties dans une poursuite et passibles de sanctions.

Bien que l'étendue de la responsabilité civile des administrateurs et des dirigeants dans le contexte des recours collectifs en matière de cybersécurité n'ait pas encore été mise à l'épreuve, les recours collectifs intentés par des investisseurs américains fournissent quelques indications quant à la mesure dans laquelle les dirigeants et les administrateurs canadiens pourraient éventuellement être tenus responsables en cas d'incidents de cybersécurité au sein de leur organisation. En particulier, ces affaires indiquent que les actionnaires d'une société peuvent avoir des recours spéciaux en vertu de la loi à l'encontre des dirigeants et des administrateurs (par exemple, lorsque ces personnes ne divulguent pas intentionnellement des informations sur les vulnérabilités en matière de cybersécurité au marché public ou tout simplement ne préviennent pas les atteintes à la

[2] Voir la norme NERC CIP-008-06, *Cyber Security — Incident Reporting and Response Planning*, à la page 14.
[3] *Pipeline Security Guidelines*.

sécurité des données). Des recours semblables d'origine législative existent actuellement au Canada et les modifications proposées à la législation fédérale sur la protection de la vie privée du Canada visent à instaurer de nouvelles sanctions et un droit d'action privé à la suite d'un constat de non-conformité à la loi. Ces modifications, si le projet de loi est adopté, peuvent accroître le risque que les administrateurs et les dirigeants soient tenus responsables dans la mesure où ils ne s'acquittent pas de leurs responsabilités en matière de cybersécurité.

Perspective de Deloitte

Comment atténuer la responsabilité par une approche holistique de la cybersécurité

Afin de lutter de manière proactive contre les cybermenaces toujours plus nombreuses dans le secteur de l'énergie, les entreprises doivent rester vigilantes face aux risques de cybersécurité, s'assurer que des contrôles appropriés de confidentialité et de cybersécurité sont en place et prendre des mesures pour remédier à toute lacune pertinente. Pour atteindre ces objectifs (et atténuer leur propre responsabilité), les dirigeants et les administrateurs en particulier doivent envisager de prendre certaines des mesures suivantes pour atténuer les risques et la responsabilité en matière de cybersécurité en s'assurant que :

- le risque de cybersécurité est un élément régulier de l'ordre du jour du conseil d'administration et des autres réunions;
- les administrateurs et les dirigeants sont au courant des risques importants en matière de cybersécurité qui concernent l'entreprise et qu'ils y sont formés;
- les administrateurs et les dirigeants posent les bonnes questions aux bonnes parties prenantes et recrutent des spécialistes externes en cybersécurité, au besoin;
- les administrateurs et les dirigeants vérifient si l'organisation a mis en place de manière appropriée :
    - des contrôles de cybersécurité (personnes, processus, technologie);
    - des capacités d'intervention en cas d'incident (guides stratégiques, avances d'honoraires);
    - des pratiques de traitement des données personnelles (conformité avec les lois sur la protection de la vie privée);
- les incidents majeurs sont transmis au conseil d'administration et les administrateurs disposent d'une stratégie d'intervention diligente qui est régulièrement mise à l'épreuve (par exemple, au moyen de simulations de crise).

Comme les entreprises d'électricité et de gaz sont particulièrement vulnérables aux cyberattaques, une approche holistique pour traiter les vulnérabilités en matière de cybersécurité peut **réduire considérablement** la responsabilité de l'organisation et des dirigeants/administrateurs. Pour répondre aux immenses problèmes juridiques, géographiques, organisationnels et techniques propres aux organisations dans ce secteur, une approche **multidisciplinaire**, **intégrée** et **innovante** offrirait aux entreprises

du secteur de l'énergie les outils et conseils suivants pour se prémunir contre les cybermenaces et les contrer :

- évaluations globales de la maturité en matière de cybersécurité afin de jauger la maturité actuelle en matière de cybersécurité, de comparer les capacités de l'organisation à celles de ses pairs du secteur et d'identifier les occasions permettant d'élaborer un modèle d'exploitation solide en matière de cybersécurité;
- état de préparation et préparation aux incidents (y compris l'élaboration de politiques de confidentialité et de cybersécurité, de plans et de protocoles d'intervention en cas d'incident, l'examen et la négociation des accords relatifs aux données (par exemple, les addendas relatifs à la protection des données, les accords d'externalisation, etc.);
- intervention en cas d'incident (y compris agir à titre de coach en cas d'atteinte à la sécurité des données, coordonner les avis/rapports sur la confidentialité et en vertu de la réglementation, engager des équipes de juricomptabilité, diriger des analyses rétrospectives et recommander des programmes d'amélioration de la protection de la vie privée et de la cybersécurité, et gérer les enquêtes réglementaires); et
- conseils juridiques sur diverses autres questions liées aux données (y compris, mais sans s'y limiter, les évaluations de confidentialité et de sécurité des données et les audits de conformité, la diligence raisonnable en matière de confidentialité et de cybersécurité dans le contexte des transactions d'entreprise et autres, la formation et la sensibilisation des employés à la confidentialité, la gouvernance des données et les pratiques de consentement lié aux renseignements).

Comment Deloitte peut-il vous aider?

L'équipe multidisciplinaire de professionnels de Deloitte S.E.N.C.R.L./s.r.l. et Deloitte Legal Canada S.E.N.C.R.L./s.r.l. peut vous aider à comprendre les vulnérabilités en matière de cybersécurité qui pourraient avoir une incidence sur votre entreprise et y répondre.

Si vous avez des questions, n'hésitez pas à contacter votre conseiller de Deloitte ou l'une des personnes-ressources indiquées dans la présente alerte.

Deloitte.

Deloitte S.E.N.C.R.L/s.r.l.
La Tour Deloitte
1190, avenue des Canadiens-de-Montréal, bureau 500
Montréal, Québec H3B 0M7
Canada

Deloitte offre des services dans les domaines de l'audit et de la certification, de la consultation, des conseils financiers, des conseils en gestion des risques, de la fiscalité et d'autres services connexes à de nombreuses sociétés ouvertes et fermées dans différents secteurs. Deloitte sert quatre entreprises sur cinq du palmarès Fortune Global 500^{MD} par l'intermédiaire de son réseau mondial de cabinets membres dans plus de 150 pays et territoires, qui offre les compétences de renommée mondiale, le savoir et les services dont les clients ont besoin pour surmonter les défis d'entreprise les plus complexes. Deloitte S.E.N.C.R.L./s.r.l., société à responsabilité limitée constituée en vertu des lois de l'Ontario, est le cabinet membre canadien de Deloitte Touche Tohmatsu Limited. Deloitte désigne une ou plusieurs entités parmi Deloitte Touche Tohmatsu Limited, société fermée à responsabilité limitée par garanties du Royaume-Uni, ainsi que son réseau de cabinets membres dont chacun constitue une entité juridique distincte et indépendante. Pour une description détaillée de la structure juridique de Deloitte Touche Tohmatsu Limited et de ses sociétés membres, voir www.deloitte.com/ca/apropos.

Notre raison d'être mondiale est d'avoir une influence marquante. Chez Deloitte Canada, cela se traduit par la création d'un avenir meilleur en accélérant et en élargissant l'accès au savoir. Nous croyons que nous pouvons concrétiser cette raison d'être en incarnant nos valeurs communes qui sont d'ouvrir la voie, de servir avec intégrité, de prendre soin les uns des autres, de favoriser l'inclusion et de collaborer pour avoir une influence mesurable.

Pour en apprendre davantage sur les quelque 330 000 professionnels de Deloitte, dont plus de 11 000 font partie du cabinet canadien, veuillez nous suivre sur LinkedIn, Twitter, Instagram ou Facebook.