La cybersécurité au temps de la COVID-19

28 avril 2020

Comme la pandémie de COVID-19 force l'adoption rapide de technologies et de modalités de télétravail, les risques en matière de cybersécurité se multiplient et s'accentuent pour les organisations de tout type et de toute taille. Il importe que ces organisations étudient et mettent en place, comme il convient, les recommandations officielles récemment publiées (voir l'annexe) pour mieux gérer les risques de cybersécurité découlant de la crise actuelle. De plus, lorsque les circonstances le permettent, il est recommandé aux organisations de profiter de l'occasion pour améliorer leur cybersécurité générale.

COVID-19 et risques informatiques

On entend par cybersécurité l'utilisation par une organisation de divers contrôles (fondés sur les personnes, les processus et les technologies) servant à gérer les risques de pertes, de coûts et d'obligations découlant d'un défaut ou d'une atteinte des systèmes de technologies de l'information utilisés par ou pour l'organisation, ou d'autres incidents qui pourraient compromettre la confidentialité, la disponibilité et l'intégrité des données en la possession ou sous le contrôle de l'organisation. La gestion des risques informatiques est importante non seulement pour des raisons commerciales valables, mais aussi pour des raisons de conformité à diverses obligations légales (notamment celles liées à la protection des renseignements personnels); elle vise également à éviter d'éventuelles poursuites judiciaires aux lourdes conséquences.

Depuis le début de la pandémie de COVID-19, de nombreuses organisations ont adopté dans l'urgence de nouvelles modalités de télétravail et pratiques administratives, et ont mis en place de nouvelles technologies de l'information (p. ex., outils de collaboration et de productivité infonuagiques, accès à distance aux systèmes de technologies de l'information et utilisation des appareils et services personnels à des fins professionnelles), souvent sans mesures raisonnables de gestion des risques informatiques ou sans contrats soigneusement négociés avec les fournisseurs de services et autres. Les cybercriminels profitent du stress, des distractions et de l'incertitude causés par ces nouvelles modalités et technologies, et de la peur et de l'incertitude causées par la pandémie même, pour s'attaquer aux technologies mal configurées ou mal utilisées en ciblant les vulnérabilités techniques et s'adonnant à diverses formes de fraude.

Les organismes gouvernementaux, de réglementation et d'autoréglementation ont publié des avertissements sur les différents risques informatiques nouveaux ou accentués découlant de la pandémie. Voici quelques exemples :

- **Hameçonnage/fraude** : Fraudes et arnaques en ligne, par courriel, messages textes ou téléphone (sites Web bidon, courriels d'hameçonnage, fraudes d'ingénierie sociale) par des fraudeurs qui se font passer pour des organisations gouvernementales, de réglementation, de soins de santé ou de bienfaisance, ou du personnel de soutien technique, ou encore qui misent sur la peur et l'incertitude causées par la pandémie.
- **Vulnérabilités techniques** : Exploitation de vulnérabilités critiques non corrigées et des mauvaises configurations des appareils, du matériel, des logiciels et des services, notamment les appareils, les systèmes et les services utilisés en télétravail.
- **Risques en lien avec les vidéoconférences** : Infiltration ou piratage (p. ex., une intrusion dans une vidéoconférence) de séances de vidéoconférence ou de conférences téléphoniques mal configurées, exploitation de liens, de fonctionnalités de partage de dossiers ou de vulnérabilités dans les applications de vidéoconférence, et attaques d'applications bureautiques à distance.
- **Rançongiciel/logiciel malveillant** : Distribution malveillante de rançongiciels ou d'autres applications mobiles ou logiciels malveillants.
- **Fraude en lien avec les mots de passe ou mauvaise utilisation de mots de passe** : Utilisation de mots de passe compromis ou courriels frauduleux.
- **Risques physiques** : Risques accrus de vol ou de perte d'appareils.
- **Erreurs** : Risques accrus d'erreurs de la part de travailleurs utilisant de nouvelles technologies et procédures.

Lignes directrices pour la gestion des risques informatiques découlant de la COVID-19

Les organismes gouvernementaux, de réglementation et d'autoréglementation ont publié des lignes directrices pour aider les organisations à gérer les risques informatiques découlant de la COVID-19 (voir l'annexe). Ces lignes directrices s'articulent autour des trois piliers fondamentaux d'un bon programme de cybersécurité : les personnes, les processus et les technologies. Voici, en bref, certaines de ces importantes recommandations :

1. LES PERSONNES

- **Culture/sensibilisation** : Sensibiliser et former tous les travailleurs à mettre en place et à entretenir une culture de confidentialité, de cybersécurité et de résilience opérationnelle, notamment en ce qui a trait aux modalités de télétravail et aux risques informatiques liés à la COVID-19.
- **Personnel des TI** : Former et inciter le personnel des TI à répondre aux demandes accrues, à accompagner le personnel dans l'utilisation des technologies et services nécessaires au télétravail, et à répondre aux tentatives d'hameçonnage ciblant le personnel des TI.
- **Signalement d 'incidents/intervention** : Former les travailleurs à signaler rapidement les incidents de cybersécurité, et former le personnel concerné à

mettre en œuvre les plans d'intervention en cas d'incident de cybersécurité lié aux modalités de télétravail.

- **Reddition de comptes/surveillance** : Assurer la bonne reddition de comptes et le signalement adéquat à la haute direction en ce qui a trait à la gestion des risques informatiques et aux incidents de cybersécurité.

2. LES PROCESSUS

- **Télétravail** : Mettre en place des processus, soutenus par des politiques et des procédures, afin de favoriser des modalités de télétravail sécuritaires et efficaces (politiques d'accès au système à distance, d'utilisation d'appareils personnels, de gestion des mots de passe et identifiants, de réunions virtuelles/vidéoconférences, de gestion des vulnérabilités et des correctifs).
- **Fraude liée aux paiements** : Mettre en place des procédures comptables et de paiement qui protègent de la fraude, notamment de la fraude par courriel.
- **Intervention en cas d 'incident** : Mettre à jour les plans d'intervention en cas d'incident pour y inclure les incidents de cybersécurité liés aux modalités et aux technologies de télétravail, ainsi que la conformité aux obligations légales de signalement, d'avis et de communication.
- **Sécurité physique** : Rehausser la sécurité physique des ordinateurs et des appareils, des supports de stockage numériques et des documents papier (notamment en prévoyant la mise au rebut sécurisée des documents papier).
- **Accès au système** : Revoir et mettre à jour périodiquement les privilèges rattachés aux comptes des systèmes de technologies de l'information.
- **Continuité des activités** : Mettre à jour et tester les plans de continuité des activités et de reprise après sinistre pour y inclure les modalités de télétravail et les services et technologies qui y sont associés.
- **Approvisionnement des TI** : Mettre à jour et adopter des politiques et des procédures pour l'approvisionnement de nouvelles technologies et de nouveaux services, qui comprennent la diligence raisonnable des fournisseurs et de leurs produits et services, la mise à l'essai des technologies et les exigences minimales pour les contrats applicables.

3. TECHNOLOGIES

- **Correctifs/mises à jour** : Configurer adéquatement les systèmes et les services de technologies de l'information (p. ex., les réseaux privés virtuels, les réseaux Wi-Fi, les services infonuagiques, les services de vidéoconférence et autres technologies de télétravail), les ordinateurs et appareils mobiles personnels, les systèmes d'exploitation et les applications logicielles, et y appliquer continuellement et automatiquement les correctifs et les mises à jour nécessaires.
- **Prévention/détection** : Utiliser des pare-feu, des logiciels antivirus, anti-programme malveillant et antihameçonnage, des écrans verrouillés protégés par un mot de passe, et des technologies de prévention/détection des intrusions adéquatement configurés sur tous les ordinateurs et appareils, y compris sur les appareils personnels utilisés à des fins professionnelles. Mettre en place une surveillance de système améliorée et des examens des registres pour favoriser la détection et l'intervention précoces en cas d'incident de cybersécurité.
- **RPV** : Utiliser des réseaux privés virtuels (RPV) sécurisés pour permettre l'accès à distance aux systèmes de TI.

- **Mots de passe/authentification multifacteur** : Privilégier les phrases et les mots de passe complexes et l'authentification multifacteur pour accéder aux ordinateurs et appareils mobiles, aux réseaux (y compris aux réseaux à domicile), aux comptes et aux services en ligne.
- **Wi-Fi** : Utiliser des réseaux Wi-Fi sécurisés (y compris les réseaux à domicile) au moyen d'identifiants de comptes administrateurs, de mots de passe d'utilisateurs et d'un protocole de sécurité rigoureux (p. ex., WPA2).
- **Vidéoconférences** : Recourir à des mesures de sécurité adéquates et à des configurations sécuritaires pour les réunions virtuelles et les conférences téléphoniques.
- **Gestion des appareils** : Se servir des logiciels de gestion des appareils mobiles pour configurer et gérer tous les ordinateurs et appareils personnels.
- **Protection des données** : Chiffrer efficacement les données en transit et au repos. Limiter ou contrôler l'utilisation de supports de stockage amovibles. Faire des copies de sauvegarde des données importantes et les stocker de façon sécuritaire.
- **Écoute clandestine** : Désactiver les assistants numériques permanents dans les environnements de télétravail.

Autres considérations

Il importe pour les organisations de vérifier si elles sont suffisamment assurées en ce qui concerne les risques informatiques, notamment ceux associés aux modalités de télétravail et aux systèmes et appareils de technologies de l'information utilisés par les télétravailleurs. Le marché de la cyberassurance évolue rapidement. À l'heure actuelle, il n'y a pas de normes en ce qui a trait aux libellés des polices, et la couverture offerte d'une police à l'autre diffère grandement. C'est pourquoi les organisations doivent se faire conseiller adéquatement à ce sujet. Consultez le bulletin de BLG intitulé *Insurance for Cybersecurity Incidents and Privacy Breaches* (en anglais).

Si la pandémie de COVID-19 cause actuellement de nombreuses perturbations sociales, d'importantes pertes financières et des pertes humaines terribles, elle donne également l'occasion aux organisations de mettre leurs ressources et leurs temps libres à profit pour améliorer leur cybersécurité générale. Lorsque les circonstances le permettent, il est recommandé aux organisations de profiter de l'occasion pour évaluer et améliorer de manière importante leurs pratiques de gestion de la cybersécurité. Les organismes gouvernementaux, de réglementation et d'autoréglementation ont publié des lignes directrices pour aider les organisations, quelles que soient leur nature ou leur taille, à améliorer leur cybersécurité. Consultez les bulletins de BLG intitulés *Cybersecurity Guidance for Small and Medium Organizations*; *Investment Funds Institute of Canada Issues Cybersecurity Guide*, Cybersecurity Framework for Ontario's *Electricity Industry*, et *Cybersecurity Guidance from Canadian Securities Administrators* (en anglais).

Les activités de gestion des risques informatiques peuvent entraîner la production de communications et de documents sensibles assujettis à des obligations de communication en cas d'enquêtes réglementaires ou de litiges liés à un incident de cybersécurité, à moins que ces communications et documents soient protégés par le secret professionnel. Les organisations devraient envisager d'adopter une stratégie relative au secret professionnel afin d'appliquer ce secret professionnel, s'il y a lieu, aux communications et documents créés dans le cadre d'activités de gestion préventive des

risques informatiques et d'intervention en cas d'incident de cybersécurité, et pour éviter les divulgations accidentelles et superflues de conseils juridiques confidentiels. Pour en savoir plus, voyez les bulletins de BLG intitulés Cyber Risk Management – Legal Privilege Strategy – Part 1, Cyber Risk Management – Legal Privilege Strategy – Part 2, *Legal Privilege for Data Security Incident Investigation Reports* et *Loss of Legal Privilege over Cyberattack Investigation Report* (en anglais).

Annexe – Lignes directrices sur la cybersécurité au temps de la COVID-19

Cliquez sur une province ci-après pour consulter ses lignes directrices.

Canada

- Centre antifraude du Canada, Alerte de bulletin! Fraude liée à la COVID-19
- Centre canadien pour la cybersécurité, *Alerte : Cybermenaces pesant sur les organismes de santé canadiens*
- Centre canadien pour la cybersécurité, Alerte : Facteurs à considérer pour l'utilisation de produits et services de vidéoconférence
- Centre canadien pour la cybersécurité, *Alerte : Pratiques exemplaires en cybersécurité pour la COVID-19*
- Centre canadien pour la cybersécurité, Alerte : Assurer sa sécurité en ligne pendant la pandémie de la COVID-19
- Centre canadien pour la cybersécurité, Alerte : Assurer sa sécurité en ligne pendant la période d'isolement liée à la COVID-19
- Centre canadien pour la cybersécurité, Alerte : La cybersécurité en mode télétravail
- Centre canadien pour la cybersécurité, Alerte : Conseils de cybersécurité pour le télétravail (ITSAP.10.116)
- Association canadienne des courtiers de fond mutuels, *Bulletin #0816-M - Cybercriminals Currently Exploiting the COVID-19 Pandemic* (en anglais)
- Organisme canadien de réglementation du commerce des valeurs mobilières, Avis 20-0061 : La COVID-19 et la cybersécurité

États-Unis (en anglais)

- Cybersecurity and Infrastructure Security Agency and United Kingdom National Cyber Security Centre, *Alert: COVID-19 Exploited by Malicious Cyber Actors*.
- Cybersecurity and Infrastructure Security Agency, *Alert: Enterprise VPN Security*
- Cybersecurity and Infrastructure Security Agency, *Risk Management for Novel Coronavirus (COVID-19)*
- Cybersecurity and Infrastructure Security Agency, *Avoiding Social Engineering and Phishing Attacks*
- Federal Bureau of Investigation, *Public Service Announcement: Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments*
- Federal Trade Commission, *Seven Coronavirus scams targeting your business*

Royaume-Uni (en anglais)

- National Cyber Security Centre, *Phishing attacks: dealing with suspicious emails and messages*
- National Cyber Security Centre, *Home working: preparing your organisation and staff*
- National Cyber Security Centre, *Video conferencing services: security guidance for organisations*
- National Cyber Security Centre, *Video conferencing services: using them securely*

Union Européenne (en anglais)

- EU Agency for Cybersecurity, *Tips for cybersecurity when working from home*
- EUROPOL, *Safe Teleworking Tips and Advice*
- EUROPOL, *How Criminals Profit from the COVID-19 Pandemic*
- EUROPOL, *Make Your Home a Cyber Safe Stronghold*

Australie (en anglais)

- Cyber Security Centre, *Cyber security is essential when preparing for COVID-19*
- Cyber Security Centre, *Threat update: COVID-19 malicious cyber activity*
- Cyber Security Centre, *COVID-19: Protecting Your Small Business*
- Cyber Security Centre, *Web Conferencing Security*
- Cyber Security Centre, *COVID-19: Cyber Security Tips When Working From Home*

Par

Services

Cybersécurité, respect de la vie privée et protection des renseignements personnels

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