Évaluez votre cyberhygiène grâce à notre liste de vérification afin de réduire les risques et les réclamations d'assurance liés à la cybersécurité

February 23, 2022

Il fut un temps où seules les grandes entreprises conservant de grandes quantités de renseignements personnels hautement confidentiels devaient se soucier de leur cybersécurité. Ce temps est révolu. En novembre 2021, le Centre canadien pour la cybersécurité annonçait que près du quart des petites entreprises canadiennes avaient été victimes d'un cyberincident depuis mars 2020, soulignant que la proportion réelle était sans doute plus élevée. Les petites et moyennes entreprises formaient en outre les deux tiers des victimes de rançongiciels connues selon les sites de « punition » (*name and shame*) au pays pour la première moitié de 2021.
(Nota : Certains des articles hyperliés sont en anglais seulement.)

Cela dit, la liste de vérification en 11 points relative à la cyberhygiène que nous vous présentons ici pourra vous aider – quelle que soit la taille de votre entreprise – à réduire les risques que l'on porte atteinte à votre cybersécurité. Si vous veillez à cerner et à éliminer les vulnérabilités de vos systèmes, de vos politiques et de vos pratiques, vous démontrerez à vos dirigeants, à vos clients, à vos fournisseurs et à vos assureurs que vous prenez les questions de cybersécurité au sérieux. De toute évidence, certains éléments de la liste engendreront des coûts, mais il ne faut pas perdre de vue le fait qu'au pays, une atteinte à la sécurité des données coûte à sa victime en moyenne 6,35 M$ CA, et que les cybercriminels frappent souvent leurs victimes plus d'une fois.

Cyberhygiène : liste de vérification

Examinez chacun des éléments suivants. Vous devriez pouvoir cocher chaque case d'un geste assuré. Si tel n'est pas le cas, il vous faut remédier à la situation. Nous serons heureux de vous aider.

☐ **Authentification multifacteur pour tous les utilisateurs** . Cette méthode permet de vérifier l'identité d'un utilisateur par une combinaison de moyens, par exemple avec un mot de passe et un jeton de sécurité, ou encore avec un porte-clé d'authentification et un logiciel de reconnaissance faciale. Sans ce type de combinaison, votre pare-feu, votre méthode de chiffrement et votre antivirus vous ne seront que de peu d'aide. Les assureurs exigent de plus en plus l'authentification multifacteur. Toutefois, la

combinaison classique du mot de passe et du code unique envoyé à un téléphone intelligent tend à perdre du terrain, les téléphones et numéros de téléphone pouvant se retrouver entre de mauvaises mains.

☐ **Logiciel de détection et de gestion des incidents pour protéger les terminaux.** Ce type de logiciel, différent des antivirus, vous permet de détecter puis d'examiner toute activité suspecte sur tous les terminaux de votre réseau.

☐ **Surveillance de la sécurité du réseau.** Cette surveillance, jumelée au logiciel de détection et de gestion des incidents, permet de repérer des comportements inhabituels et de confirmer s'il s'agit ou non d'activités suspectes. Si votre pare-feu a été compromis ou que vous n'en avez pas installé un, le rapport d'activité de votre outil de surveillance de réseau vous permettra de découvrir s'il y a eu préparation de données en vue d'un transfert ou d'un vol de données.

☐ **Formation régulière en matière de cybersécurité comprenant la simulation d'attaques**. La simulation d'une cyberattaque pour observer la réponse de son équipe face à la menace est aussi utile que l'exercice d'incendie pour tester l'efficacité du processus d'évacuation en cas d'urgence. Ceci vous sera utile dans votre rôle à la direction des TI ou à titre de responsable de la protection de la vie privée, puisque vous pourrez alors voir si vos employés comprennent leurs responsabilités et saisissent les risques associés à leurs comportements, ou s'il faut leur donner davantage de formation. Votre équipe interne est peut-être apte à fournir elle-même la formation sur la cybersécurité, mais, déjà très sollicitée, elle pourrait s'en trouver surchargée. BLG peut vous suggérer des formateurs externes qui correspondent à vos besoins et à votre budget; il vous suffit de communiquer avec Eric Charleston ou Julie Gauthier.

☐ **Modification et complexité obligatoires des mots de passe** . La plupart des gens choisissent des mots de passe trop simples, et ils les conservent trop longtemps. L'élément le plus important de cet énoncé est donc le mot « obligatoire ». Assurez-vous que votre système de changement du mot de passe impose la modification régulière et exige un certain niveau de complexité, pour que ces facteurs soient automatisés plutôt que de dépendre d'un individu.

☐ **Politiques précisant la manière et le moment de la mise à jour des logiciels et du matériel informatique.** Il est très important de se doter de politiques officielles à ce sujet et de ne pas compter sur des pratiques informelles de mise à jour ou sur des correctifs ponctuels.

☐ **Accès restreint aux droits d'administrateur système.** Ce type d'accès ne devrait être octroyé que lorsque nécessaire afin de réduire au minimum le nombre d'employés pouvant être victimes d'une fraude ou en position d'en commettre une.

☐ **Cartographie de données illustrant avec exactitude toute l'information à disposition** . Une telle cartographie expose l'ensemble des données que vous collectez, y compris les données anonymisées que vous stockez pour comprendre vos groupes démographiques et vos marchés. Il s'agit d'un outil, et non d'un simple document. Il vous permettra de savoir si vous recueillez trop de données, vous les conservez trop longtemps et, en cas d'accès illicite, ce qui a été consulté et volé. En cas de vol, votre assureur s'attendra à voir clairement dans votre cartographie la quantité et le type de données qui ont été compromises; s'il y trouvait des divergences, il pourrait refuser

votre réclamation. Nous pouvons procéder psi our vous au mappage des données et à l'analyse des lacunes pour vous aider d'une part à vous doter d'un plan de gestion de crise et d'une politique sur la protection de la vie privée solides, et d'autre part à vous conformer à la réglementation.

☐ **Politique de conservation des données.** Le référentiel de données d'une entreprise ne cesse de s'accroître et peut en soi poser problème. Vous devriez ne conserver que les données qu'il vous est permis de garder compte tenu de la raison initiale de leur collecte, ainsi que celles dont vous avez besoin pour produire des documents obligatoires, comme les déclarations fiscales. N'hésitez pas à vous tourner vers un·e avocat·e pour comprendre vos obligations relatives à la conservation des données et au respect de la vie privée, y compris en ce qui a trait à l'anonymisation des données. Eric Charleston, Julie Gauthier et les autres membres de l'équipe nationale Cybersécurité, respect de la vie privée et protection des renseignements personnels de BLG se feront un plaisir d'évaluer votre situation avec vous.

☐ **Sauvegarde des données hors site** . Vos données doivent être sauvegardées sur des serveurs qui ne sont pas reliés à votre réseau. Elles peuvent être stockées sur un disque dur ou dans le nuage. Dans tous les cas, l'emplacement des serveurs doit être conforme aux exigences relatives au respect de la vie privée.

☐ **Programme visant la protection des renseignements personnels.** Les lois relatives à la protection des renseignements personnels varient d'un pays à l'autre, voire d'un endroit à l'autre au sein d'un même pays – et elles sont en constante évolution. La loi québécoise sur la protection des renseignements personnels, adoptée en septembre 2021, a marqué un tournant sur le plan de la responsabilisation et de l'application de la loi au pays. Chaque entreprise doit se doter d'un programme qui régit et dirige l'utilisation de ses données, en fonction de son domaine d'activité, du type de données qu'elle collecte, conserve, traite et transfère, de ses obligations contractuelles et réglementaires, des risques associés à ses données ainsi que de ses principes touchant la protection des renseignements personnels. Les notions de consentement doivent faire partie de ce programme. Les entreprises du secteur privé qui procèdent à la collecte de renseignements personnels des Canadiens et Canadiennes doivent se conformer aux lignes directrices canadiennes relatives au consentement.

Voilà qui conclut notre liste de vérification de la cyberhygiène. Avez-vous pu cocher les 11 cases? Si oui, félicitations, votre cyberhygiène est irréprochable – à tout le moins pour le moment. N'oubliez pas toutefois que le domaine des technologies de l'information progresse rapidement, et que les cybercriminels rivalisent d'ingéniosité; cette liste de vérification, tout comme vos habitudes de cyberhygiène, devra toujours évoluer.

Si vous n'avez pu cocher certaines des cases, ne vous inquiétez pas; saisissez plutôt l'occasion pour améliorer votre cyberhygiène en parant à vos vulnérabilités par des décisions éclairées. L'équipe Cybersécurité, respect de la vie privée et protection des renseignements personnels de BLG peut vous aider à trouver les bons fournisseurs de service, à cerner vos obligations contractuelles et réglementaires et à comprendre comment vous collectez, utilisez et stockez vos données, de façon à ce que vos habitudes de cyberhygiène deviennent aussi naturelles pour vous que celles de vous laver le visage et de vous brosser les dents.

Par :

Eric S. Charleston, Julie M. Gauthier

Services :

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

---

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

BLG Offices

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 De La Gauchetière Street West
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