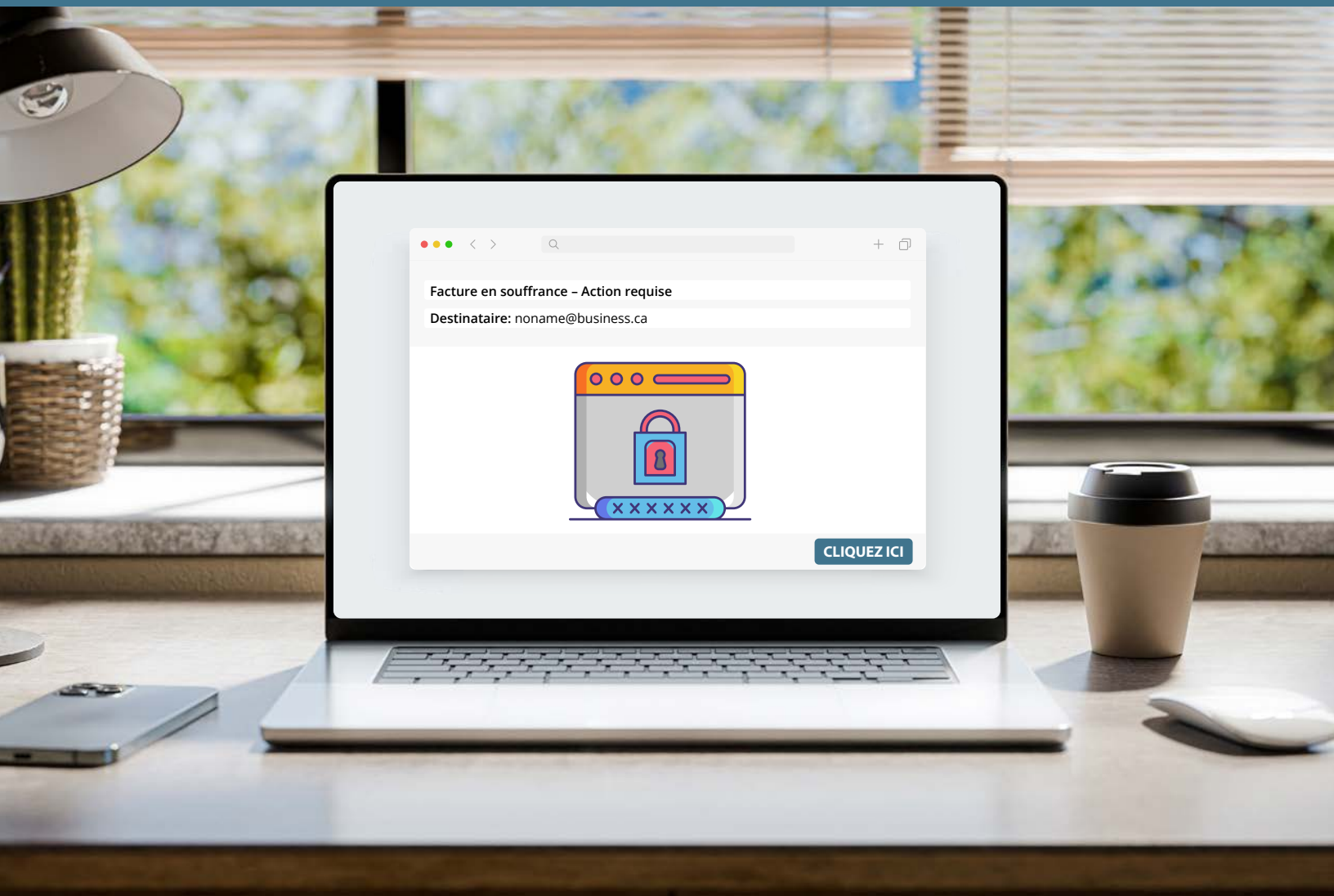
cyberaverti

Les cybercriminels adorent les petites entreprises

Apprenez comment mieux protéger votre petite entreprise avec ce guide d'assurance pour les cyberavisés



Protégez mieux votre entreprise de la cybercriminalité

Une seule violation des données pourrait coûter à votre entreprise jusqu'à **7 millions de dollars**. C'est le plus récent chiffre canadien tiré du rapport d'IBM de 2025. Pour une PME, il ne s'agit pas d'une seule facture. **Il s'agit d'un ensemble de coûts :** les frais dispendieux de l'embauche de spécialistes en TI pour corriger l'incident, les frais juridiques en cas de poursuite par un client, les amendes des organismes de réglementation et les pertes de ventes pendant un arrêt des systèmes.

Il suffit d'un seul clic. Ce qui semble être une facture jointe à un courriel ou une alerte de sécurité pourrait plonger votre entreprise dans une véritable crise avec des pertes financières, des poursuites et une réputation ternie.

Votre entreprise y survivrait-elle?

La cybercriminalité est un marché lucratif et encore plus efficace grâce aux outils de l'intelligence artificielle. Il est plus important que jamais pour les entreprises et les organisations de prendre des mesures proactives pour s'en protéger.

Grâce à ce manuel, vous apprendrez à élaborer un solide plan de cybersécurité et à protéger votre entreprise avec le bon contrat d'assurance contre les cyberrisques, ce qui vous donnera une stratégie de défense fiable.

Le Canada se classe au deuxième rang dans le monde parmi les pays les plus touchés par les attaques de rançongiciels, avec 216 victimes au premier semestre de 2025.

***Toronto Star*, 5 août 2025**

Ai-je besoin de la cyberassurance?

Comme propriétaire d'entreprise, vous disposez sans doute déjà d'une couverture d'assurance pour vos activités, notamment une assurance responsabilité civile générale, une assurance de dommages et peut-être même une assurance responsabilité professionnelle. Ces contrats d'assurance vous protègent contre les préjudices physiques, les créances légales et les risques opérationnels. En revanche, elles ne couvrent généralement pas grand-chose des risques numériques, comme la violation de données, les perturbations technologiques et la cyberextorsion. C'est là où le contrat de cyberassurance entre en jeu.

Adoptons cette perspective : imaginez qu'un voleur s'introduit dans votre bureau durant la nuit. Une assurance pour entreprises traditionnelle vous aiderait à couvrir les coûts liés à la porte cassée et à l'équipement volé.

Et si un voleur ne brise pas votre porte, mais s'introduit dans vos systèmes électroniques? Il pourrait voler vos données confidentielles, vous empêcher d'accéder à votre propre réseau et exiger une rançon, voire causer une panne des systèmes qui interrompra vos activités. La plupart des contrats traditionnels ne couvrent pas toujours ce type de risques numériques. C'est là l'utilité de la cyberassurance : elle est conçue pour vous protéger d'une effraction par voie numérique.

Que couvre habituellement l'assurance contre les cyberrisques?

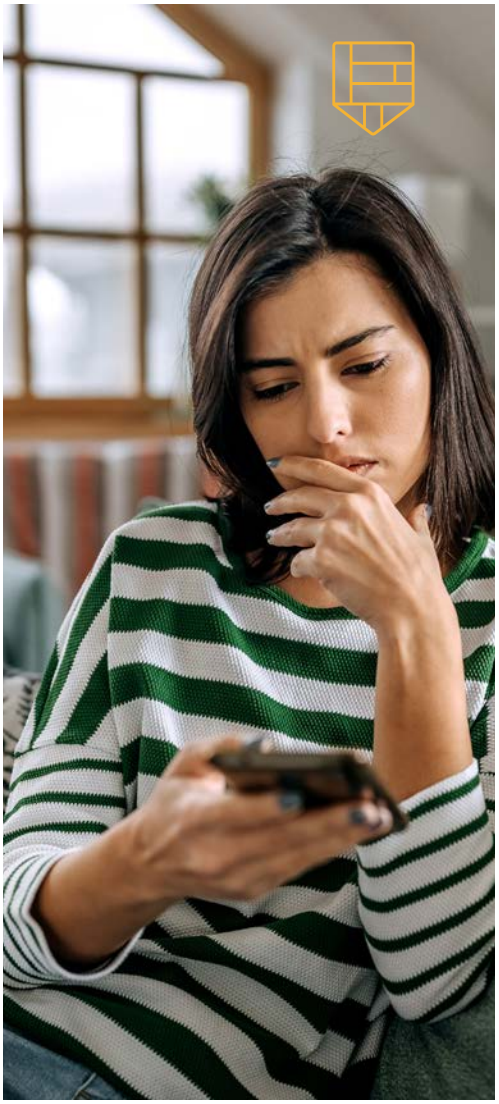
La cyberassurance peut couvrir les pertes découlant d'un éventail de cyberévénements, notamment :

- La perte, la divulgation ou la consultation non autorisée de renseignements confidentiels ou personnels;
- Une défaillance technologique ou une attaque par déni de service;
- Une demande de paiement accompagnée de menaces visant vos données, comme l'interruption de vos activités ou la compromission de vos renseignements confidentiels.

Cette liste n'est pas exhaustive, puisque la couverture en cybersécurité peut varier d'un assureur à l'autre et évolue constamment. Vous pouvez travailler avec votre représentant en assurance pour trouver la couverture qui répondra à vos besoins.

La cyberassurance peut vous aider à couvrir les coûts associés à des cyberévénements, notamment :

- La notification des parties concernées;
- L'atténuation du préjudice potentiel découlant de toute atteinte à la vie privée, comme la surveillance du crédit des personnes concernées;
- La compréhension de ce qui s'est passé : il faudra faire appel à un expert en cybercriminalité pour déterminer la cause fondamentale et la portée de la violation des données;
- Les frais juridiques et les dommages civils liés à une atteinte à la vie privée ou à la sécurité du réseau.



Il y a généralement trois types de cyberassurance :

- À l'heure actuelle, les contrats de cyberassurance autonomes (ceux dédiés entièrement aux cyberrisques) constituent l'option la plus complète disponible au Canada, et ils se distinguent de tout autre contrat d'assurance que vous pourriez avoir.
- Un contrat d'assurance terrestre conventionnel qui peut comporter une couverture limitée pour certains cyberévénements. Une cybercouverture pour ces types de contrats est généralement limitée de telle sorte qu'elle pourrait ne pas couvrir le coût total d'une atteinte ou d'une cyberattaque.
- Les avenants (un type de couverture complémentaire) peuvent ajouter, retirer ou exclure certaines cybercouvertures, modifiant ainsi un contrat de cyberassurance ou un contrat d'assurance conventionnel pour répondre à des besoins précis.

Bien qu'un solide plan de cybersécurité puisse bloquer de nombreuses menaces, aucune défense n'est parfaite. Une assurance contre les cyberrisques vous protège en cas d'attaque. La première étape pour obtenir la bonne couverture consiste à comprendre vos risques propres et à commencer à élaborer votre plan.

Votre entreprise risque-t-elle une cyberattaque?

Étant donné que votre entreprise est unique, elle peut avoir un niveau de cyberrisque différent de celui d'autres entreprises.

Même si les entreprises peuvent être exposées au risque dans une certaine mesure, celles qui gèrent les données de nature délicate sur les clients, traitent les paiements en ligne ou dépendent fortement de l'infrastructure numérique sont tout particulièrement à risque. Plus les enjeux sont élevés, plus le besoin d'une cybersécurité et d'une protection en assurance robustes est élevé.

Vous êtes peut-être plus à risque que vous ne le pensez. Voici des exemples de question à vous poser pour déterminer votre risque :

- Sauvegardez-vous une liste de courriels de clients sur une plateforme de marketing en ligne?
- Traitez-vous les ventes à l'aide d'un fournisseur de services de paiement?
- Conservez-vous les dossiers d'employés (p. ex. les numéros d'assurance sociale pour la paie) sur un ordinateur?

Si vous avez répondu oui à l'une des questions ci-dessus, vous traitez des données sensibles.

Pour connaître certaines des forces et faiblesses possibles de votre entreprise et sa disposition à repousser une cyberatteinte, répondez au questionnaire Autoévaluation de la cyberassurance (en anglais) du Bureau d'assurance du Canada (BAC). Les 10 questions qui vous sont posées vous aideront à en apprendre plus sur les protocoles et les pratiques exemplaires en matière de cybersécurité que la plupart des cyberassureurs prennent en compte lors de l'évaluation du risque. Le questionnaire comporte également certaines des questions que les assureurs utilisent déjà dans leur processus de demande.

Par exemple, on vous demandera de prendre en compte ce qui suit :

- La collecte et le stockage des renseignements personnels des clients, le cas échéant;
- Les procédures de sécurité en place;
- La fréquence à laquelle une formation en cybersécurité est donnée au personnel.

Ces questions s'apparentent à celles qui pourraient figurer sur une demande de cyberassurance.

Même si cet outil gratuit ne permet pas d'obtenir une évaluation proprement dite du risque, il peut vous aider à déterminer si vous êtes un bon candidat pour la cyberassurance et à établir les secteurs sur lesquels votre entreprise doit se concentrer pour renforcer la cybersécurité.

Vous trouverez l'autoévaluation sur

CyberSavvyCanada.ca

Comment puis-je présenter une demande de cyberassurance?

Si vous envisagez la cyberassurance pour votre entreprise, vous auriez vraisemblablement à remplir une demande que les assureurs pourraient utiliser pour évaluer les risques pour votre entreprise et tarifer votre contrat.

Pour vous aider à vous préparer en conséquence, voici des exemples de ce qu'on pourrait vous demander lors de la présentation de votre demande :

Comment décririez-vous votre entreprise?

1. Comment décririez-vous les activités de l'organisation?
2. Combien d'employés ou de travailleurs contractuels comptent votre ou vos organisations? Indiquez le nombre d'employés par service.
3. Qui sont vos clients? Sont-ils des consommateurs, des fonctionnaires ou des employés d'autres entreprises?

Quels renseignements votre entreprise recueille-t-elle et est-ce une exigence de les collecter? Plus particulièrement, combien de dossiers de la liste conservez-vous au sein de votre organisation?

1. Numéros de compte de cartes de débit et de crédit
2. Données financières pour autrui
3. Pièces d'identité délivrées par un gouvernement (permis de conduire, passeports, numéros d'assurance sociale)
4. Renseignements personnels : nom, adresse et coordonnées de particuliers
5. Renseignements médicaux ou sur la santé de particuliers
6. Secrets commerciaux ou propriété intellectuelle
7. Renseignements d'entreprise d'autres organisations

CONSEIL : Envisagez de réduire la quantité de renseignements que vous recueillez pour réduire les risques de violation de la vie privée.

Quels plans et protocoles de sécurité sont en place dans votre entreprise actuellement?

1. Avez-vous rédigé un plan d'information ou de sécurité en matière de protection de la vie privée pour l'organisation? Ce plan respecte-t-il la réglementation gouvernementale en place pour le traitement et la divulgation de renseignements personnels ou confidentiels?
2. Quand la dernière évaluation de sécurité ou de protection de la vie privée a-t-elle été effectuées? Les recommandations s'y rapportant ont-elles toutes été mises en œuvre? Pourquoi une ou plusieurs recommandations n'ont-elles pas été mises en œuvre, le cas échéant?
3. Offrez-vous une formation sur la cybersécurité ou la protection de la vie privée à tous les membres du personnel?

Quelles mesures de cybersécurité sont en place pour aider à réduire les cyberrisques pour votre entreprise?

1. Quelles mesures physiques sont appliquées pour empêcher l'accès aux installations ou aux bureaux?
2. Quelles mesures de sécurité sont appliquées actuellement pour empêcher l'accès aux systèmes de TI et aux serveurs?
3. Quelle technologie est utilisée aux fins de chiffrement et d'authentification? De quel logiciel antivirus et de quels pare-feu votre entreprise dispose-t-elle?

Vous trouverez l'autoévaluation sur

CyberSavvyCanada.ca

Qu'arrivera-t-il si je communique des renseignements à mes fournisseurs? Pourrais-je être poursuivi s'ils perdaient mes données?

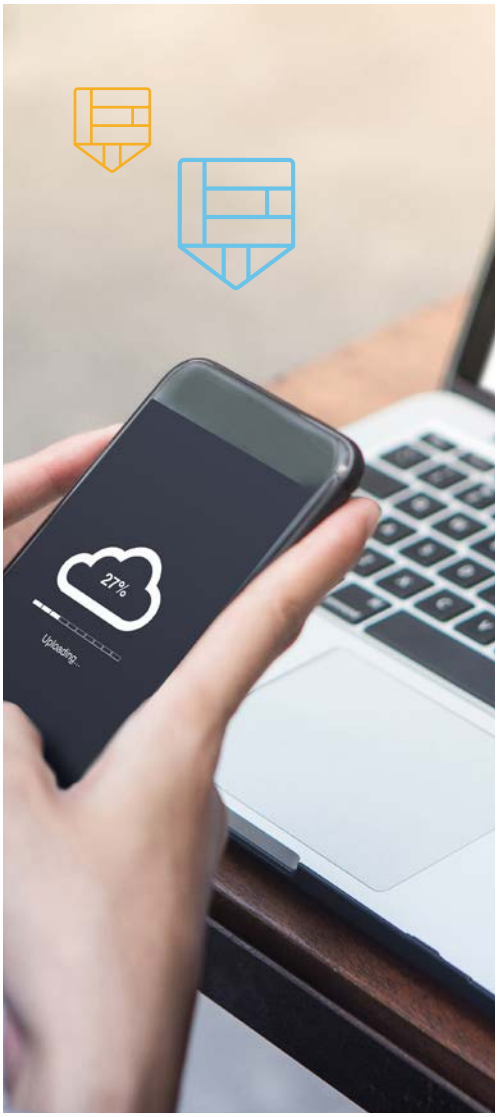
Comme propriétaire d'entreprise, vous devez vous assurer de protéger des données sensibles, même lorsqu'elles sont entre les mains de tiers, notamment vos fournisseurs. Par exemple, vous pourriez être tenu responsable de tout dommage portant atteinte à vos clients si vous communiquez les renseignements de vos clients à une société de logiciels qui se fait pirater. La bonne nouvelle, c'est que vous pouvez gérer ce risque et prendre des mesures pour mieux protéger votre organisation.

Une étape clé consiste à leur faire remplir un questionnaire sur leurs pratiques en matière de cybersécurité. Les questions doivent porter notamment sur des renseignements commerciaux, comme le nom de la société de portefeuille ou de la société mère, l'emplacement physique du fournisseur et le lieu de stockage de ses systèmes et données.

Le questionnaire doit également permettre de réévaluer les pratiques du fournisseur en matière de gestion du risque.

Par exemple, il peut comporter les questions suivantes :

- Le fournisseur dispose-t-il d'un plan de gouvernance du risque et d'une évaluation du risque officiels?
- Les sous-traitants ont-ils accès aux données ou aux installations du fournisseur?
- Le fournisseur a-t-il désigné une personne ou une équipe qui assure la supervision et la mise en œuvre de la cyberformation de son personnel et une politique de sécurité?



Pour plus de rigueur, il est également recommandé de demander des documents justificatifs à l'appui des réponses fournies une fois que vous aurez examiné les réponses du fournisseur.

Assurez-vous de réévaluer le rendement de vos fournisseurs en les soumettant de temps à autre à des mesures de cybersécurité et tenez des dossiers à jour de tous les fournisseurs qui procurent des services à votre entreprise.

Dans certains cas, vous devriez intégrer les fournisseurs à vos plans d'intervention en cas de cyberincident et y indiquer les processus de notification des atteintes et les listes de vos contacts clés.

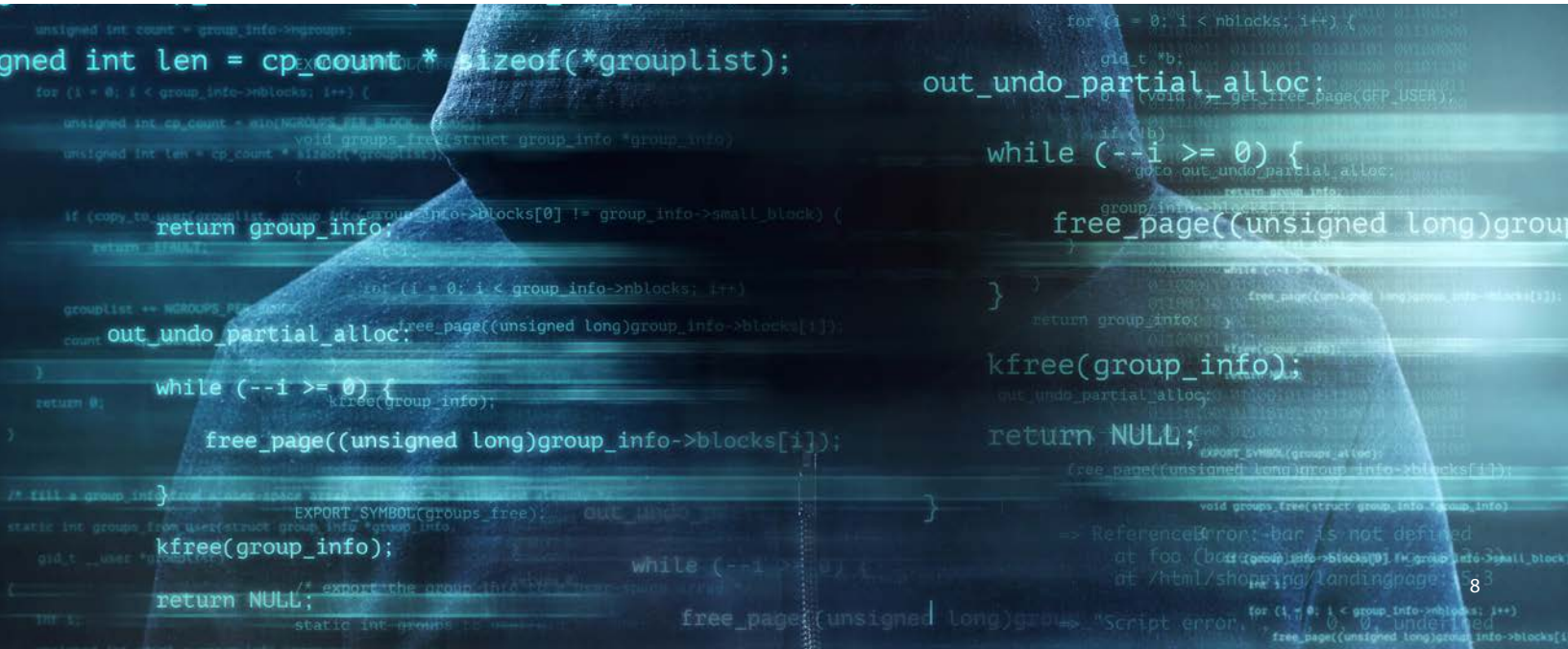
Pensez à mettre en place des processus de gestion de fin de contrat pour les fournisseurs dont les contrats se terminent, afin de vous assurer qu'ils n'ont plus accès à vos systèmes ou à vos données. Si cela est nécessaire, assurez-vous qu'ils détruisent les dossiers de nature délicate.

Pire scénario : Ce qu'il faut faire immédiatement après une cyberattaque

Malheureusement, les cybercrimes peuvent toujours survenir, et ce, malgré tous vos efforts. Si votre entreprise est victime d'un cybercrime, votre meilleure défense sera d'agir rapidement. **Si vous êtes victime d'une brèche de sécurité, préparez-vous-y maintenant en suivant les étapes essentielles suivantes :**

- Changez les mots de passe et questions de sécurité du compte compromis et de tous les comptes connexes.
- Déterminez quelles données ont été touchées, par exemple les renseignements financiers ou personnels. Incluez-y toute exposition à l'étranger : les réseaux et les données assujettis à la réglementation étrangère comme le *Règlement général sur la protection des données* (RGPD).
- Voyez si des renseignements personnels sur la santé (RPS) peuvent avoir été recueillis ou compromis.
- Intégrez des mesures de sécurité avancées comme la détection et l'intervention au point d'extrémité (EDR) et l'authentification multifacteur (AMF) pour gérer l'accès des employés.
- Signalez l'incident…
    - À votre cyberassureur, qui pourra vous aider avec les étapes à suivre pour protéger vos données;
    - Au fournisseur de compte de même qu'aux fournisseurs des comptes connexes;
    - À la police;
    - Au Centre canadien pour la cybersécurité (contact@cyber.gc.ca) pour le signalement du vol d'identité organisationnel;
    - Au *Centre antifraude du Canada* en ligne ou au 1 888 495-8501 s'il s'agit d'un vol d'identité;
    - À Innovation, Sciences et Développement économique Canada si vous détenez des renseignements sur des logiciels malveillants, des menaces électroniques ou des pourriels.

Sources : Centre canadien pour la cybersécurité et Innovation, Sciences et Développement économique Canada



Comment votre assureur peut vous aider à reprendre vos activités après une cyberattaque

Une cyberattaque est un événement complexe que peu d'entreprises peuvent gérer seules. Votre représentant en assurance peut vous aider en vous fournissant des renseignements sur un réseau de spécialistes en reprise des activités après une atteinte à la sécurité et l'accès à ce réseau. Votre contrat de cyberassurance pourrait même couvrir tout ou partie des coûts d'un cyberincident, de la prévention à la reprise des activités en passant par le confinement.

Voici quelques-unes des façons qu'un contrat de cyberassurance peut aider votre entreprise à réduire l'impact d'une attaque et à reprendre ses activités :

- Votre assureur peut vous mettre en contact avec des experts autorisés, comme une équipe de réseautage et d'ingénierie des données, ou exiger que vous fassiez appel à eux, pour déterminer quels renseignements ont été compromis. Certains de ces contrats globaux peuvent couvrir ces frais d'experts.
- Les compagnies d'assurance tiennent souvent une liste de leurs fournisseurs de services de confiance. L'accès à cette liste peut vous aider à accélérer le processus consistant à faire appel aux spécialistes qui s'imposent afin que vous évitiez de perdre un temps précieux à déterminer les services dont vous avez besoin et les personnes qualifiées pour vous les offrir.
- Un contrat d'assurance complète peut couvrir certaines dépenses découlant d'une cyberattaque, notamment les frais juridiques et les règlements dans le cadre des poursuites intentées par des tiers pour les clients touchés, sous réserve de conditions et limites. Il pourrait également couvrir certaines dépenses de spécialistes pour vous aider à rétablir la réputation de votre entreprise et à regagner la confiance des clients.

Protégez votre organisation des cyberrisques

Tout le monde a un rôle à jouer dans la réduction des cybermenaces au travail. Même si la cyberassurance est un important filet de sécurité pour une entreprise en cas de cyberatteinte, elle doit être considérée seulement comme un élément d'une vaste stratégie d'atténuation des cyberrisques visant à réduire la vulnérabilité de l'organisation aux menaces en ligne.

La cyberprotection n'a pas besoin d'être coûteuse ni complexe. Si vous suivez les conseils ci-dessous de *Pensez cybersécurité*, cela pourra vous aider à augmenter votre cybersécurité :

- ***Créez une politique en matière de cybersécurité.*** Fixez des règles claires sur la façon dont votre équipe traite les données et les appareils.
- ***Formez votre équipe.*** Montrez à vos employés comment reconnaître les pourriels et donnez-leur la possibilité d'appliquer régulièrement des pratiques sécuritaires en ligne.
- ***Utilisez des outils de sécurité de catégorie entreprise.*** Protégez vos systèmes en optant pour un logiciel antivirus et des pare-feu professionnels.
- ***Protégez votre réseau.*** Verrouillez votre Wi-Fi et séparez vos systèmes de TI sensibles de tout système auquel le public a accès.

- ***Sauvegardez les données essentielles.*** Enregistrez régulièrement vos données, conformément aux lois applicables. (Remarque : Assurez-vous de respecter les exigences de votre province concernant l'endroit où les données peuvent être stockées et sauvegardées.)
- ***Limitez l'accès aux renseignements sensibles.*** Donnez aux employés un accès seulement aux renseignements nécessaires à l'exercice de leurs fonctions.
- ***Tenez le logiciel et les systèmes à jour.*** Installez toujours des versions actualisées pour corriger les failles de sécurité.
- ***Utilisez l'authentification multifacteur (AMF).*** Ajoutez une protection supplémentaire pour l'ouverture de session, en plus des mots de passe.
- ***Protégez les appareils mobiles.*** Définissez de forts paramètres de sécurité sur les téléphones et les tablettes que les employés utilisent au travail.
- ***Créez un plan d'intervention en cas d'incident.*** Préparez un guide détaillé pour la gestion des cyberattaques.

Apprenez-en plus avec le

Guide Pensez cybersécurité pour les petites entreprises

Création d'un plan de cybersécurité

La création d'un plan est une étape importante que les petites et moyennes entreprises peuvent suivre pour les aider à être plus résilientes par rapport aux cyberatteintes et à réduire leur cyberrisque dans l'ensemble.

Commencez par déterminer les renseignements et les systèmes utiles, comprendre les principales menaces et appliquer les pratiques exemplaires en matière de gestion du risque pour votre entreprise.

La liste de contrôle ci-dessous du *Centre canadien pour la cybersécurité* présente les mesures à prendre en compte dans la création de votre cyberplan.

- ***Créez un plan d'intervention en cas d'incident.*** Si vous avez un plan, vous pouvez répondre rapidement aux incidents, restaurer les données et les systèmes essentiels et limiter les interruptions de service et les pertes de données.
- ***Corrigez les systèmes et les applications.*** Lorsque des problèmes ou des vulnérabilités de logiciels sont relevés, les vendeurs de logiciels distribuent des correctifs pour réparer les bogues, remédier aux vulnérabilités connues et améliorer la convivialité ou le rendement.
- ***Utilisez une forte authentification de l'utilisateur.*** Appliquez des politiques d'authentification de l'utilisateur qui marient sécurité et convivialité. Assurez-vous que vos appareils professionnels authentifient les utilisateurs avant que ceux-ci puissent accéder à vos systèmes. Utilisez autant que possible l'AMF.
- ***Sauvegardez et chiffrez vos données.*** Copiez vos renseignements opérationnels et vos applications essentielles dans un ou plusieurs emplacements comme le nuage ou un disque dur externe. (Remarque : Veillez à ce que vos sauvegardes soient effectuées conformément aux lois applicables en matière de protection des renseignements personnels et de données.)
- ***Activez le logiciel de sécurité.*** Activez les pare-feu et installez les logiciels antivirus et anti-programmes malveillants sur tous vos appareils professionnels pour contrecarrer les attaques malveillantes et vous protéger contre les maliciels.
- ***Formez vos employés.*** Personnalisez vos programmes de formation pour y inclure des renseignements sur les protocoles, les politiques et les procédures de sécurité de votre organisation. Un personnel informé peut réduire la probabilité de cyberincidents.

Protégez les services infonuagiques et impartis. Apprenez à connaître un fournisseur de services avant de lui confier des contrats.

Protégez les sites Web. Protégez votre site Web et les renseignements sensibles qu'il recueille. Chiffrez les données sensibles, assurez-vous que vos certificats sont à jour, utilisez des phrases de passe ou des mots de passe forts dans le programme d'arrière-plan du site et utilisez le protocole https dans l'adresse de votre site.

Protégez les appareils mobiles. Choisissez un modèle de déploiement des appareils. Ainsi, les employés utilisent seulement les applications approuvées et téléchargent uniquement les applications de sources fiables sur les appareils qu'ils utilisent au travail.

Maintenez le contrôle et l'autorisation d'accès pour les employés. Appliquez le principe de privilège minimal afin de contribuer à prévenir l'accès non autorisé et les atteintes à la sécurité des données. Autrement dit, les employés devraient avoir accès uniquement aux renseignements requis dans l'exercice de leurs fonctions.

Établissez des mesures de défense de base du périmètre. Défendez vos réseaux des cybermenaces. Par exemple, utilisez un pare-feu pour vous défendre contre les intrusions externes en surveillant le trafic entrant et sortant et en filtrant les activités malveillantes.

Configurez les appareils en toute sécurité. Prenez le temps de revoir les paramètres de tous les appareils utilisés pour mener vos activités; n'utilisez jamais de mot de passe par défaut et apportez des modifications au besoin.

Protégez les dispositifs multimédias portables. Même si un dispositif multimédia portable comme une clé USB peut s'avérer pratique et rentable pour stocker et transférer des données, il est susceptible d'être perdu ou volé.

Téléchargez la liste de contrôle complète à

CyberSavvyCanada.ca

Liste de contrôle de Cyber Savvy

N'ignorez pas les risques de cybermenaces pour votre petite ou moyenne entreprise. Être cyberavisé, ça commence par l'application des pratiques exemplaires en matière de cybersécurité.

Bien que la meilleure solution soit de parler à un spécialiste en cyberassurance en sécurité des diverses stratégies qui s'appliquent à votre entreprise, répondre aux questions de la liste de contrôle ci-dessous peut vous aider à mieux déterminer si vous prenez les bonnes mesures de protection de votre entreprise contre les cyberrisques.

Avec quels cyberrisques votre entreprise doit-elle composer actuellement?

Une autoévaluation de votre entreprise constitue la première étape dans la création d'un plan de cybersécurité durable et efficace. Vous devez d'abord comprendre les systèmes, les actifs, les données et les capacités de votre entreprise afin de pouvoir déterminer et gérer le risque lié à la cybersécurité.

Votre entreprise prend-elle les bonnes mesures pour se protéger contre les cyberrisques?

Avez-vous appliqué les mesures de protection appropriées pour gérer la sécurité de vos systèmes et données?

Votre entreprise sait-elle comment détecter les cybermenaces?

Les procédures de surveillance et de détermination de l'occurrence d'un incident de cybersécurité sont-elles en place?

Avez-vous un plan d'intervention en cas de cybermenaces?

Avez-vous un plan d'intervention présentant les procédures que votre entreprise doit suivre lors de la détection d'un incident de cybersécurité?

Avez-vous un plan pour aider votre entreprise à reprendre ses activités à la suite d'une cyberattaque?

Avez-vous indiqué les activités qui doivent être exécutées pour rétablir les capacités ou les services touchés en raison d'un incident de cybersécurité et pour maintenir des plans aux fins de résilience?

Téléchargez la liste de contrôle complète à CyberSavvyCanada.ca

À propos du Bureau d'assurance du Canada

Établi en 1964, le Bureau d'assurance du Canada (BAC) est l'association industrielle nationale qui représente les assureurs privés d'habitation, d'automobile et d'entreprise du Canada. Ses sociétés membres constituent la grande majorité du marché fortement concurrentiel de l'assurance de dommages au Canada.

À titre de défenseur des assureurs de dommages privés au Canada, le BAC collabore avec les gouvernements, les organismes de réglementation et les intervenants pour soutenir un environnement concurrentiel afin que l'industrie de l'assurance de dommages continue de protéger les Canadiens des risques auxquels ils sont exposés aujourd'hui et seront exposés à l'avenir.

Le BAC est d'avis que les Canadiens valorisent et méritent une industrie de l'assurance de dommages privée sensible et résiliente qui offre des solutions d'assurance tant aux particuliers qu'aux entreprises.

Pour plus d'information, accédez à **bac.ibc.ca**. Suivez-nous sur **LinkedIn**, **X** et **Instagram**, et aimez-nous sur **Facebook**. Si vous avez des questions au sujet de l'assurance habitation, automobile ou entreprise, n'hésitez pas à communiquer avec le Centre d'information des consommateurs du BAC, au 1 844 227-5422. Nous sommes là pour vous aider.

bac.ibc.ca

Ce guide est offert en format accessible sur demande. Vous n'avez qu'à envoyer un courriel à info@cybersavvycanada.ca.