



2727 COWORKING / RECHERCHE ET CONSEILS PRATIQUES

Cyberassurance des petites entreprises : les mesures de sécurité d'abord

Find a practical home for your work at 2727 Coworking in Montreal. Explore private offices, day workspaces and meeting rooms, plus business-address and virtual-mailbox services for your company.

Publié par 2727 Coworking · 2026-10-29 · cyberassurance petites entreprises Canada · cybersécurité petites entreprises Canada
contrôles de base · hameçonnage petites entreprises Canada

Article original : <https://2727coworking.com/articles/fr/cyberassurance-petites-entreprises-mesures-securite-dabord>

Dans cet article

1. Pourquoi les mesures de sécurité passent avant l'assurance
2. Étape 1 : Les 13 contrôles de base du Centre pour la cybersécurité
3. Étape 2 : À quoi sert une police de cyberassurance
4. Étape 3 : Les questions que les assureurs vous poseront
5. Étape 4 : Les questions à poser avant de signer
6. Étape 5 : Les obligations légales au Québec après un incident
7. Un plan de départ sur 30 jours

Pourquoi les mesures de sécurité passent avant l'assurance

Les petites entreprises commencent généralement à penser à la cyberassurance après avoir eu une bonne frousse : le compte de courriel d'un client est piraté, un portable est volé, une demande de rançon apparaît sur le lecteur partagé. À ce moment-là, la première question de l'assureur n'est pas « Quel montant de protection voulez-vous? », mais « Quelles mesures de sécurité avez-vous en place? »

Les chiffres laissent croire que la plupart des petites entreprises ne sont pas prêtes à répondre à cette question. Dans un sondage commandé par le Bureau d'assurance du Canada (BAC) et publié le 1er octobre 2025, seulement 47 % des répondants de petites et moyennes entreprises affirmaient que leur entreprise était prête à faire face à une cyberattaque ou à une atteinte à la sécurité des données, moins de la moitié (48 %) avaient mis en place une quelconque forme de cyberdéfense, à peine 22 % détenaient une cyberassurance et seulement 12 % avaient une police distincte consacrée aux cyberrisques (BAC, octobre 2025). Le même communiqué cite une étude de BDC selon laquelle 73 % des petites entreprises ont subi un incident de cybersécurité.

Ce guide commence par les préparatifs qui ne coûtent rien : les contrôles de base du Centre canadien pour la cybersécurité, un organisme fédéral. Il explique ensuite les frais qu'une police de cyberassurance prend habituellement en charge, les questions des assureurs et les obligations légales au Québec qui s'appliquent, que vous ayez une assurance ou non.

Cet article fournit des renseignements généraux et ne constitue pas un conseil en assurance ni un avis juridique.

Étape 1 : Les 13 contrôles de base du Centre pour la cybersécurité

Le Centre canadien pour la cybersécurité publie les *Contrôles de cybersécurité de base pour les petites et moyennes organisations* (version 1.2). Son objectif déclaré est d'appliquer « the 80/20 rule (achieve 80% of the benefit from 20% of the effort) » à la cybersécurité des petites et moyennes organisations ([Centre pour la cybersécurité, contrôles de base](#)). Le document présente 13 contrôles :

#	Contrôle	Ce que cela signifie pour une entreprise de 1 à 10 personnes
3.1	Élaborer un plan d'intervention en cas d'incident	Un plan d'une page précisant « qui appelle qui », rédigé avant qu'un incident survienne
3.2	Appliquer automatiquement les correctifs aux systèmes d'exploitation et aux applications	Activer les mises à jour automatiques partout; remplacer les appareils et les logiciels que le fournisseur ne prend plus en charge
3.3	Activer les logiciels de sécurité	Un logiciel antimaliciel qui se met à jour et effectue des analyses automatiquement; des pare-feu intégrés activés
3.4	Configurer les appareils de façon sécuritaire	Changer les mots de passe par défaut, désactiver les fonctions inutilisées
3.5	Utiliser une authentification forte des utilisateurs	L'authentification à deux facteurs partout où c'est possible
3.6	Offrir une formation de sensibilisation aux employés	Reconnaître les courriels et les liens malveillants, adopter de bonnes habitudes en matière de mots de passe
3.7	Sauvegarder et chiffrer les données	Des sauvegardes régulières des données essentielles, chiffrées, avec des copies hors ligne
3.8	Sécuriser la mobilité	Déterminer à qui appartiennent les téléphones et comment ils sont protégés
3.9	Établir des mesures de défense de base du périmètre	Protéger les réseaux connectés à Internet, en commençant par un pare-feu
3.10	Sécuriser les services infonuagiques et les services informatiques externalisés	Savoir ce que vos fournisseurs protègent et ce que vous devez protéger
3.11	Sécuriser les sites Web	Protéger le site et les données qu'il traite
3.12	Mettre en place le contrôle des accès et les autorisations	Appliquer le principe du moindre privilège; retirer les accès dont les personnes n'ont plus besoin

#	Contrôle	Ce que cela signifie pour une entreprise de 1 à 10 personnes
3.13	Sécuriser les supports amovibles	Les clés USB et les cartes SD se perdent facilement; les chiffrer ou éviter de les utiliser

Ces conseils s'adressent aux organisations qui n'ont pas une grande équipe informatique, et les recommandations le précisent. Par exemple, pour l'application des correctifs, le document recommande aux petites et moyennes organisations de « enable automatic updates for all software and hardware if such an option is available - or consider replacing products with ones that provide the option, » plutôt que d'adopter les programmes complets de gestion des correctifs qu'il conseille aux grandes entreprises (même source).

Les cinq contrôles les plus avantageux pour une petite équipe

1. L'authentification à deux facteurs (3.5). Le Centre pour la cybersécurité recommande l'authentification à deux facteurs « wherever possible, » et indique que les organisations devraient l'exiger pour les comptes importants, comme les comptes financiers, en consignant chaque cas où elles décident de ne pas le faire. Il recommande aussi de changer les mots de passe seulement lorsqu'on soupçonne une compromission ou qu'on en a la preuve, plutôt qu'à intervalles fixes (même source). Commencez par les courriels, les services bancaires, la paie, le logiciel de comptabilité et votre registraire de noms de domaine.

2. Des sauvegardes avec une copie hors ligne (3.7). Les contrôles de base recommandent de sauvegarder régulièrement les renseignements essentiels de l'entreprise dans un emplacement externe sécurisé, de conserver les sauvegardes chiffrées avec un accès restreint et d'envisager un stockage hors ligne dans un lieu sécurisé à l'extérieur des locaux, ou de consigner les raisons de ne pas le faire. Ils précisent que les sauvegardes à long terme (par exemple, hebdomadaires) doivent être hors ligne, tandis que les sauvegardes fréquentes (par exemple, quotidiennes) peuvent être en ligne (même source). Un dossier synchronisé dans le nuage n'est pas une sauvegarde si un rançongiciel peut aussi le chiffrer.

3. Les mises à jour automatiques (3.2). Activez-les sur les portables, les téléphones, les routeurs et les navigateurs. Remplacez le vieux routeur qui ne reçoit plus de mises à jour.

4. La formation de sensibilisation (3.6). Les contrôles de base énumèrent des sujets pratiques : les politiques sur les mots de passe, la reconnaissance des courriels et des liens malveillants, les logiciels approuvés, l'utilisation appropriée d'Internet et l'utilisation sécuritaire des médias sociaux (même source). Une séance de 30 minutes par année, accompagnée d'une règle exigeant de confirmer par téléphone tout changement aux renseignements de paiement, permet de parer à la plupart des tentatives de fraude à la facture.

5. Un plan d'intervention en cas d'incident (3.1). Le Centre pour la cybersécurité conseille de tenir pour acquis que des incidents surviendront et de prévoir un plan d'intervention et de rétablissement dans le cadre de la planification de la continuité des activités (même source). Notre [modèle de plan de continuité des activités pour petites entreprises](#) comporte une section que vous pouvez adapter.

Si votre équipe travaille à distance ou dans des espaces partagés, notre [liste de vérification de la sécurité en télétravail](#) applique ces contrôles aux réseaux domestiques et au Wi-Fi public.

Étape 2 : À quoi sert une police de cyberassurance

Une police de cyberassurance prend en charge les coûts que les mesures de sécurité n'ont pas permis d'éviter. Pensez cybersécurité, la campagne fédérale de sensibilisation, et le BAC énumèrent les coûts qu'une police de cyberassurance distincte peut aider à couvrir ([Pensez cybersécurité](#)) :

Catégorie de garantie	Ce qu'elle prend en charge
Restauration des systèmes réseau et des données électroniques	La restauration ou la récupération des données endommagées ou corrompues après une atteinte à la sécurité, une attaque par déni de service ou une attaque par rançongiciel
Mesures correctives et avis à la suite d'une atteinte à la sécurité	Les avis aux personnes touchées et l'atténuation des préjudices, par exemple la surveillance du crédit
Enquête informatique judiciaire	Les services d'une firme chargée d'enquêter sur la cause et l'étendue d'une atteinte à la sécurité
Frais juridiques et dommages-intérêts civils	La représentation juridique et les éventuels dommages-intérêts liés à une atteinte à la vie privée ou à la sécurité du réseau

Le BAC décrit les risques de façon plus large : les pertes liées aux atteintes à la sécurité des données personnelles, à la cyberextorsion, aux perturbations technologiques et à d'autres risques ([BAC, Votre petite entreprise est-elle admissible à la cyberassurance?](#)).

Pourquoi votre assurance d'entreprise actuelle peut être insuffisante

Le BAC est clair dans ses conseils : « most property or liability policies don't expressly cover cyber risks, or have very limited coverage, » de sorte qu'il peut être pertinent d'envisager une police de cyberassurance distincte, en complément des mesures préventives (même page du BAC). Si vous avez déjà une assurance responsabilité civile des entreprises ou une police multirisque, demandez par écrit à votre courtier lesquelles des quatre catégories ci-dessus elle couvre et jusqu'à quel montant. Notre [guide d'assurance pour les travailleurs autonomes](#) explique les autres assurances qu'une petite entreprise détient habituellement.

Étape 3 : Les questions que les assureurs vous poseront

Le BAC a créé un outil gratuit d'autoévaluation de 10 questions qui aide les propriétaires à se renseigner sur les protocoles de sécurité et les pratiques exemplaires que recherchent la plupart des assureurs en cyberassurance, et qui pose certaines des questions que les assureurs pourraient poser lors de la demande. Il invite notamment les propriétaires à réfléchir à leurs cyberrisques, à la collecte et à la conservation des renseignements personnels de leurs clients, à leurs procédures de sécurité et à la fréquence des formations des employés sur la cybersécurité. Le BAC précise que l'outil « cannot provide an actual risk assessment, » mais qu'il peut aider à évaluer le degré de préparation ([BAC](#)).

Avant d'appeler un courtier, préparez des réponses à des questions comme celles-ci, associées aux contrôles de base :

Question probable dans la demande	Contrôle de base	Vos pièces justificatives
L'authentification à deux facteurs est-elle activée pour les courriels et l'accès à distance?	3.5	Capture d'écran des paramètres d'administration
À quelle fréquence faites-vous des sauvegardes, et une copie est-elle hors ligne?	3.7	Calendrier des sauvegardes, date du dernier test de restauration
Les appareils sont-ils mis à jour automatiquement?	3.2	Liste des appareils avec les versions des systèmes d'exploitation
Les employés reçoivent-ils une formation en sécurité?	3.6	Date de la dernière séance, présences
Avez-vous un plan d'intervention en cas d'incident?	3.1	Le document du plan
Conservez-vous des renseignements personnels sur vos clients? Où?	3.10, 3.12	Inventaire des données
Qui a des droits d'administration?	3.12	Liste des comptes d'administration

Répondez honnêtement. La valeur d'une police dépend de l'exactitude des renseignements fournis dans la demande; si vos mesures de sécurité ne sont pas encore en place, il vaut généralement mieux les mettre en œuvre avant de présenter une demande.

Étape 4 : Les questions à poser avant de signer

Le libellé des polices varie, et aucune source publique ne définit une police de cyberassurance type pour les petites entreprises. Voici les questions à poser à votre courtier :

1. Lesquelles des quatre catégories de garantie (restauration des données, avis, enquête informatique judiciaire, frais juridiques et dommages-intérêts) sont incluses, et quelle est la limite de chacune?
2. Y a-t-il une franchise ou un délai de carence avant que la garantie contre les pertes d'exploitation entre en vigueur?
3. La police couvre-t-elle l'ingénierie sociale ou la fraude à la facture (un client qui paie un fraudeur après avoir reçu un faux courriel)?
4. Couvre-t-elle les incidents chez vos fournisseurs de services infonuagiques ou informatiques?
5. Quelles mesures de sécurité sont des conditions de la garantie (par exemple, l'authentification à deux facteurs doit être activée)?
6. L'assureur offre-t-il une ligne d'urgence en cas d'incident, et devez-vous faire appel à ses fournisseurs?
7. La police couvre-t-elle les enquêtes réglementaires et les coûts des avis aux personnes exigés par la loi québécoise?

Étape 5 : Les obligations légales au Québec après un incident

Qu'elle soit assurée ou non, une entreprise québécoise qui détient des renseignements personnels a des obligations légales lorsqu'un problème survient. En vertu de la *Loi sur la protection des renseignements personnels dans le secteur privé* (P-39.1, [LégisQuébec](#)) :

- **Ce qui constitue un incident.** Un « confidentiality incident » est un accès, une utilisation ou une communication de renseignements personnels non autorisés par la loi, ou la perte de renseignements personnels ou toute autre atteinte à leur protection (art. 3.6). La Commission d'accès à l'information (CAI) donne notamment comme exemples un employé qui consulte des renseignements sans autorisation, l'envoi de renseignements au mauvais destinataire et une cyberattaque comme l'hameçonnage ou un rançongiciel (CAI, [Incidents de confidentialité](#)).
- **Agir pour limiter les préjudices.** Si vous avez des motifs de croire qu'un incident s'est produit, vous devez prendre des mesures raisonnables pour diminuer les risques de préjudice et éviter que de nouveaux incidents de même nature se produisent (art. 3.5).
- **Aviser lorsque le risque est sérieux.** Si l'incident présente un risque de préjudice sérieux, vous devez aviser avec diligence la CAI et les personnes dont les renseignements sont concernés (art. 3.5). Pour évaluer ce risque, vous devez tenir compte de la sensibilité des renseignements, des conséquences appréhendées de leur utilisation et de la probabilité qu'ils soient utilisés à des fins préjudiciables, et consulter la personne responsable de la protection des renseignements personnels (art. 3.7).
- **Tenir un registre.** Vous devez tenir un registre des incidents de confidentialité et en transmettre une copie à la CAI à sa demande (art. 3.8). Cette obligation s'applique à tous les incidents, pas seulement aux incidents sérieux.
- **Les fournisseurs ne vous dégagent pas de vos obligations.** La CAI indique qu'une entreprise qui confie des renseignements personnels à un tiers demeure responsable de ses obligations en cas d'incident : mesures, registre et avis ([CAI](#)).

La CAI suggère d'évaluer rapidement un incident à l'aide de six questions : qui est touché, combien de personnes, quels renseignements sont concernés, quand l'incident s'est produit et a été découvert, où (au sein de l'entreprise ou chez un fournisseur) et pourquoi les mesures de sécurité ont échoué (même page de la CAI). Intégrez ces questions à votre plan d'intervention en cas d'incident.

Si vous n'avez pas encore mis en place les autres mesures de conformité à la Loi 25, commencez par notre [liste de vérification de la conformité à la Loi 25 pour les microentreprises](#).

Un plan de départ sur 30 jours

Semaine	Actions
1	Activer l'authentification à deux facteurs pour les comptes de courriel, de services bancaires, de comptabilité et de noms de domaine. Dresser la liste de tous les comptes d'administration.
2	Activer les mises à jour automatiques sur tous les appareils. Remplacer les routeurs ou les portables qui ne sont plus pris en charge. Configurer des sauvegardes chiffrées avec une copie hebdomadaire hors ligne; tester une restauration.
3	Rédiger un plan d'intervention en cas d'incident d'une page, en y intégrant les six questions de la CAI et le nom de la personne qui tient le registre des incidents. Tenir une séance de sensibilisation à l'hameçonnage de 30 minutes.
4	Remplir l'autoévaluation du BAC, rassembler les pièces justificatives du tableau ci-dessus et demander des soumissions à un courtier. Comparer les libellés, pas seulement les prix.

Liens vers les sources

Liens cités dans cet article, dans leur ordre de première apparition. Les adresses complètes sont fournies pour les lecteurs qui utilisent le texte extrait.

1. <https://www.ibc.ca/news-insights/news/canadian-small-businesses-are-underprepared-for-cyber-attacks-survey-shows>
2. <https://www.cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations>
3. <https://www.getcybersafe.gc.ca/en/blogs/cyber-insurance-can-help-reduce-online-risks-businesses-all-sizes>
4. <https://www.ibc.ca/news-insights/in-focus/does-your-small-business-qualify-for-cyber-insurance>
5. <https://www.legisquebec.gouv.qc.ca/en/document/cs/P-39.1>
6. <https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privees/incidents-confidentialite-mesures-securite-entreprises>

L'ÉDITEUR

À propos de 2727 Coworking

2727 Coworking is a Montreal workspace and business-address provider. We serve people who need a place to focus, meet, run a small business or establish a professional mailing presence. Our website offers English and French information about workspace options and services, alongside educational resources for operating a business in Canada.

A workspace that fits the day

Our workspace options include private offices, day passes and desks, and a conference room. These formats help individuals and teams compare a dedicated office with more flexible ways to work or hold a meeting. Prospective members can explore the virtual tour, review current pricing and book a visit before choosing a workspace.

Business addresses and mail

2727 Coworking provides business-address and virtual-mailbox services. Our resources explain the documents and practical questions involved, including guidance for people outside Canada. Service eligibility, included features, availability and access arrangements should be confirmed on the applicable service page or with our team.

Resources for Canadian small businesses

We publish guides, research and planning tools about workspace decisions, business addresses and starting a business in Canada. Our incorporation research includes information for people inside Canada and abroad, with jurisdiction-specific material to help readers identify the next questions to investigate. These educational resources complement our workspace and address services; they are not individualized legal, tax or immigration advice.

Visit or contact 2727 Coworking

Explore [private offices](#), [day passes and desks](#), [the conference room](#), [business addresses](#) and [virtual mailboxes](#). [Book a visit](#) or [contact the team](#) to discuss your needs.

A business address alone does not establish tax residence, immigration status, banking approval or eligibility for a government program.

Site Web : <https://2727coworking.com>

Cet article est de nature informative. Validez toute décision médicale, juridique, financière, réglementaire ou technique importante auprès de professionnels compétents et des sources primaires citées. Les services de l'entreprise sont décrits séparément des constats de recherche de l'article.