

Avant de signer votre proposition d'assurance cyber

Ce que chaque question de sécurité vous engage à affirmer, où les réponses de bonne foi dérapent, et une autovérification de 30 minutes avant de signer.

Lecture de 9 minutes

Autovérification de 30 minutes

Mis à jour en octobre 2026

Ce que chaque question de sécurité vous engage réellement à affirmer, où les gens de bonne foi se font prendre, et quoi vérifier avant de signer.

POURQUOI C'EST PLUS IMPORTANT QUE LA PRIME

La proposition n'est pas un sondage. Elle fait partie du contrat, et vous signez une déclaration attestant que vos réponses sont exactes.

- **Au Québec**, le Code civil (art. 2408 à 2411) vous oblige à déclarer toutes les circonstances connues de vous qui sont de nature à influencer de façon importante l'assureur dans l'établissement de la prime, l'appréciation du risque ou la décision de l'accepter. Si une réponse se révèle inexacte, l'assureur peut demander la nullité du contrat s'il ne vous aurait pas assuré en connaissant les faits. En l'absence de fraude, il peut plutôt réduire l'indemnité en proportion de la prime qu'il aurait dû exiger. Vos réponses doivent aussi demeurer exactes pendant la durée du contrat : vous devez déclarer promptement à l'assureur les changements qui aggravent le risque (art. 2466).
- **Ailleurs au Canada**, les lois provinciales sur les assurances et le libellé des polices vont dans le même sens : une fausse déclaration importante peut annuler la couverture.
- **Ce que ça donne en pratique** : dans l'affaire *Travelers c. International Control Services* (États-Unis, 2022), l'assuré avait déclaré que l'authentification multifacteur protégeait les accès administratifs et privilégiés. Après une attaque par rançongiciel, Travelers a allégué que l'authentification multifacteur ne protégeait que le pare-feu. ICS a accepté l'annulation rétroactive de la police, comme si elle n'avait jamais existé, et le tribunal a rejeté l'action. L'affaire s'est réglée sans jugement sur le fond, et c'est une décision américaine, mais le mécanisme est le même ici. La réponse qui fait perdre la réclamation est habituellement un « oui » qui était vrai pour *certaines* systèmes seulement.

La règle que nous donnons à nos clients : répondez en fonction de votre système le plus faible, pas du meilleur. Si la vraie réponse est « en grande partie », répondez « non » et joignez une explication. Un « non » assorti d'une date de correction peut faire augmenter votre prime, ajouter une exclusion ou mener à un refus. Un faux « oui » peut anéantir votre couverture après l'incident.

LES QUESTIONS ET LEURS PIÈGES

Les formulations ci-dessous reprennent des tournures courantes dans les propositions d'assurance cyber. Le libellé de votre assureur sera différent : lisez le sien mot à mot. *(Les citations sont traduites de l'anglais; la proposition française de*

1. Authentification multifacteur

Libellé type : « Authentification multifacteur imposée pour sécuriser **tous** les accès à distance à votre réseau. »
« Authentification multifacteur imposée pour sécuriser l'utilisation interne des comptes privilégiés (comptes administrateurs, **comptes de service**, etc.). » « Authentification multifacteur imposée pour l'accès au courriel par le portail Web, les applications de messagerie et les **appareils n'appartenant pas à l'entreprise**, pour tous les employés. »

Les pièges

- ◇ « **Tous les accès à distance** » inclut votre fournisseur de services gérés et vos fournisseurs. L'outil de gestion à distance de votre fournisseur TI (ConnectWise, N-able, TeamViewer, AnyDesk), le compte RPV du fournisseur de ventilation-climatisation ou de comptabilité, le vieux bureau à distance « temporaire » ouvert pour un consultant : si l'un d'eux entre sans authentification multifacteur, la réponse est non. Demandez par écrit à votre fournisseur de services gérés comment son accès chez vous est protégé.
- ◇ L'« accès à distance » dépasse le RPV. Un assureur le définit comme l'accès à « un appareil, un service Web d'entreprise ou un réseau, à partir de n'importe quel endroit ». Les applications infonuagiques accessibles de la maison comptent.
- ◇ Certaines connexions au courriel contournent encore l'authentification multifacteur. SMTP AUTH avec un simple mot de passe (souvent laissé actif pour des numériseurs, des imprimantes ou une application d'affaires), les mots de passe d'application, Exchange sur site et le courriel hébergé ailleurs que chez Microsoft 365 ou Google peuvent tous accepter un mot de passe sans second facteur. « Authentification multifacteur sur le courriel » n'est vrai que si ces accès sont désactivés ou limités à des appareils désignés.
- ◇ Comptes de service et comptes d'urgence (bris de glace). Les propositions posent la question des comptes privilégiés « y compris les comptes de service ». La plupart des petits environnements ont au moins un compte administrateur de domaine ou un compte de service de sauvegarde sans authentification multifacteur, avec un mot de passe inchangé depuis des années.
- ◇ Les certificats et les clés partagées ne sont pas de l'authentification multifacteur. Au moins un assureur précise que l'authentification multifacteur moderne « n'inclut pas les méthodes d'authentification statiques comme les certificats ou les clés prépartagées ».
- ◇ « Imposée » veut dire une politique, pas une simple inscription. Si les utilisateurs se sont inscrits, mais qu'une exception d'Accès conditionnel les exclut (le PDG, « parce que c'est fatigant »), la réponse est fausse.

Autovérification : exportez votre rapport d'inscription à l'authentification multifacteur et vos politiques d'Accès conditionnel (ou l'application obligatoire de la validation en deux étapes de Google). Dressez la liste de toutes les exclusions. Dressez la liste de tous les moyens par lesquels une personne de l'extérieur atteint un appareil de votre réseau. Vérifiez si SMTP AUTH est activé quelque part dans votre locataire.

2. Sauvegardes

Libellé type : des cases à cocher comme « Une copie des sauvegardes est conservée **hors ligne** ou **isolée physiquement (air gap)** », « Solution de sauvegarde avec sauvegardes **immuables** », « Les serveurs de sauvegarde **ne sont pas joints à un domaine Windows** », « **Authentification multifacteur exigée** pour accéder aux sauvegardes », « Les serveurs de sauvegarde et les comptes utilisateurs utilisent des **identifiants distincts** ».

Les pièges

- ◇ **Hors ligne, immuable et infonuagique sont trois réponses différentes.** *Hors ligne* = déconnectée, donc hors de portée de l'attaquant. *Immuable* = en ligne, mais impossible à modifier ou à supprimer avant une date de conservation, même par un administrateur. *Infonuagique* = stockée ailleurs, ce qui ne dit rien sur la possibilité de la supprimer avec un mot de passe administrateur volé. Un NAS Synology sur le même réseau, avec une copie programmée sur disque USB, n'est rien de tout ça.
- ◇ **Serveurs de sauvegarde joints au domaine.** Si le serveur de sauvegarde s'authentifie avec le même Active Directory dont l'attaquant vient de prendre le contrôle, l'attaquant contrôle aussi les sauvegardes. C'est une méthode courante des groupes de rançongiciel pour supprimer les sauvegardes avant de chiffrer.
- ◇ **« Testée » veut dire une restauration, pas un crochet vert.** Les souscripteurs demandent de plus en plus quand vous avez fait votre dernière restauration, et combien de temps elle a pris. Un logiciel de sauvegarde qui affiche « tâche réussie » n'est pas un test de restauration.
- ◇ **Données SaaS.** La conservation dans Microsoft 365 et Google Workspace n'est pas une sauvegarde au sens où l'entendent les assureurs. Si vos fichiers sont dans SharePoint ou OneDrive, précisez comment ils sont sauvegardés.

Autovérification : un mot de passe d'administrateur de domaine peut-il supprimer vos sauvegardes? Dans le doute, supposez que oui. Quand avez-vous restauré un serveur complet pour la dernière fois, et combien de temps cela a-t-il pris? Notez la date et la durée.

3. Protection des postes et serveurs (EDR / MDR)

Libellé type : « Quelle technologie de sécurité des terminaux avez-vous en place? Antivirus nouvelle génération / Détection et réponse sur les terminaux (EDR) / Détection et réponse gérées (MDR) / Détection et réponse étendues (XDR) », avec un champ pour nommer le produit et le fournisseur. D'autres assureurs demandent si l'EDR est déployé sur **tous** les postes et serveurs, et si les alertes sont **surveillées 24/7**.

Les pièges

- ◇ **L'EDR est un outil; la surveillance 24/7 est un service.** Si la question dit « surveillées 24/7 » et que les alertes arrivent dans la boîte de courriel de votre responsable TI, la réponse est non. Un « oui » à la surveillance 24/7 suppose un fournisseur MDR, ou un fournisseur de services gérés doté d'un vrai centre des opérations de sécurité (SOC) en service jour et nuit. Faites-le inscrire au contrat.
- ◇ **« Tous les terminaux » veut dire tous.** Comparez le nombre d'appareils dans la console EDR avec votre inventaire. L'écart se trouve presque toujours du côté des serveurs (surtout le vieux serveur auquel personne ne touche), et c'est là que les attaquants débarquent.
- ◇ **Defender n'est pas automatiquement un EDR.** Antivirus Microsoft Defender, inclus dans Business Basic/Standard, n'est pas Defender for Endpoint ni Defender for Business. Vérifiez la licence, pas le logo.
- ◇ **Nommez le produit correctement.** Les souscripteurs comparent le nom du produit avec la liste de ce qu'ils considèrent comme un EDR.

Autovérification : nombre d'appareils dans l'EDR ÷ nombre total d'appareils (serveurs compris) = __ %. Qui reçoit l'alerte à 3 h du matin un dimanche? Un nom, pas « le fournisseur ».

4. Bureau à distance exposé et équipements périphériques

Libellé type : « Permettez-vous l'accès à distance par RDP? » / « Le RDP est-il exposé à Internet? » Certains assureurs sautent la question et **vous balayent de l'extérieur** avant de vous soumettre une offre : un port RDP exposé ressortira, peu importe votre réponse.

Les pièges

- ◇ **L'assureur connaît peut-être déjà la réponse.** Si vous répondez « pas de RDP » et que son balayage trouve le port 3389 ouvert sur une adresse IP que vous aviez oubliée, une fausse déclaration figure à votre dossier avant même que vous signiez.
- ◇ **Le boîtier RPV compte aussi.** Les pare-feu et les appareils RPV non corrigés (Fortinet, SonicWall, Cisco, Ivanti, Citrix) comptent parmi les portes d'entrée les plus exploitées des dernières années. C'est précisément pour ça que les assureurs posent des questions sur l'application des correctifs.

Autovérification : regardez-vous de l'extérieur avant que l'assureur le fasse. Une évaluation des vulnérabilités vous montre ce qu'il verra.

5. Correctifs et systèmes en fin de vie

Libellé type : « En combien de temps les correctifs critiques sont-ils appliqués? » « Utilisez-vous des logiciels non pris en charge ou en fin de vie? »

Les pièges

- ◇ **Votre politique de correctifs est jugée sur le pire appareil.** Le serveur Windows Server 2012 qui fait rouler le vieux logiciel comptable, ou un poste Windows 10 dont le soutien a pris fin (octobre 2025), rend fausse la réponse « aucun logiciel non pris en charge ». Les exceptions : les appareils inscrits aux mises à jour de sécurité étendues (ESU) de Microsoft, ou ceux qui sont isolés et déclarés.
- ◇ **Le micrologiciel compte.** Les pare-feu, les RPV, les NAS et les imprimantes sont des « systèmes ».

Autovérification : dressez la liste de tous les systèmes dont le système d'exploitation ou le micrologiciel n'est plus pris en charge. Pour chacun : inscrit aux ESU? Isolé? Date de remplacement?

6. Formation et hameçonnage

Libellé type : « Offrez-vous une formation en sécurité ou une formation sur l'hameçonnage à tous les employés, au moins une fois par année? »

Le piège : « tous les employés » inclut le propriétaire et les employés à temps partiel. Conservez les preuves de participation; c'est ce qu'on vous demandera.

7. Vérification des paiements

Libellé type : « Avant d'effectuer un paiement électronique, vérifiez-vous la validité de la demande de transfert de fonds ou de modification de paiement auprès du demandeur, par un moyen de communication distinct? »

Les pièges

- ◇ **Appeler le numéro inscrit dans le courriel n'est pas un moyen distinct.** La vérification doit se faire à un numéro que vous aviez déjà en dossier.
- ◇ **La règle doit s'appliquer à tout le monde, y compris au patron.** La fraude par compromission de courriel d'affaires fonctionne justement en se faisant passer pour le patron qui « a besoin que ce soit fait tout de suite ».
- ◇ **La fraude par ingénierie sociale est souvent soumise à une sous-limite.** Bien des polices plafonnent les pertes liées à la fraude au paiement bien en deçà de la limite principale, ou les excluent en l'absence de procédure de vérification. Lisez la section sur le transfert de fonds ou l'ingénierie sociale, et sa limite.

Autovérification : la règle de rappel est-elle écrite, et votre commis aux comptes fournisseurs l'appliquerait-il si le propriétaire lui disait de s'en passer?

8. Incidents antérieurs et « connaissance »

Libellé type : « Au cours des trois dernières années, avez-vous subi un incident de cybersécurité... » et « Avez-vous... connaissance d'une atteinte à la sécurité, réelle ou alléguée... susceptible de donner lieu à une réclamation? »

Les pièges

- ◇ **Une compromission de courriel d'affaires antérieure ou une boîte de courriel compromise compte comme un incident,** même si aucun argent n'a été transféré et que personne ne l'a signalée.
- ◇ **La « connaissance » est large.** Si les TI ont signalé des connexions suspectes le mois dernier, déclarez-les. Un incident connu mais non déclaré est l'un des motifs les plus nets de refus d'une réclamation.
- ◇ **Votre registre des incidents de confidentialité (Loi 25) documente ce que vous saviez.** La Commission d'accès à l'information peut l'exiger, et il peut ressortir lors d'un litige sur une réclamation. Si un incident est à votre registre, il devrait figurer dans votre proposition.

AUTOVÉRIFICATION AVANT LA PROPOSITION (30 MINUTES AVEC VOTRE FOURNISSEUR TI)

Répondez à chaque point avec une preuve, pas de mémoire.

- 1 ☐ Authentification multifacteur imposée sur toutes les boîtes de courriel, et accès par mot de passe seul (SMTP AUTH, mots de passe d'application, anciens serveurs) désactivés ou restreints. **Preuve** : export des politiques d'Accès conditionnel + liste des exclusions (vide, ou limitée aux comptes d'urgence).
- 2 ☐ Authentification multifacteur sur tous les accès au réseau, y compris les outils du fournisseur de services gérés et les comptes des fournisseurs. **Preuve** : inventaire écrit des accès à distance et de la protection de chacun.
- 3 ☐ Authentification multifacteur sur tous les comptes administrateurs, y compris les comptes de service et d'urgence. **Preuve** : liste des comptes privilégiés.
- 4 ☐ Au moins une copie de sauvegarde qu'un mot de passe d'administrateur de domaine volé ne peut pas supprimer (hors ligne ou immuable, identifiants distincts, authentification multifacteur sur la console). **Preuve** : capture d'écran des paramètres d'immuabilité ou de verrouillage de la conservation.
- 5 ☐ Une restauration complète testée au cours des 12 derniers mois. **Preuve** : date, système, durée de la restauration.
- 6 ☐ EDR sur 100 % des postes de travail *et des serveurs*. **Preuve** : nombre dans la console comparé à l'inventaire.
- 7 ☐ Surveillance 24/7 assurée par un fournisseur nommé, si vous l'affirmez. **Preuve** : contrat MDR ou SOC.
- 8 ☐ Aucun RDP, SMB ou panneau d'administration exposé à Internet; équipements périphériques à jour. **Preuve** : balayage externe.
- 9 ☐ Systèmes non pris en charge répertoriés, isolés ou inscrits aux ESU, avec dates de remplacement.
- 10 ☐ Formation annuelle pour tout le personnel, avec preuves de participation.
- 11 ☐ Règle de rappel écrite pour les paiements et les changements de coordonnées bancaires.
- 12 ☐ Tous les incidents des 3 dernières années (y compris les boîtes de courriel compromises) répertoriés en vue de leur déclaration.
- 13 ☐ Plan d'intervention en cas d'incident qui contient la ligne d'urgence de l'assureur (voir notre fiche de la première heure).

Une case que vous ne pouvez pas cocher : répondez « non » et joignez une courte note avec une date de correction. Les souscripteurs voient des « non, réglé d'ici le 31 mars » tous les jours. Un « oui » qu'ils réfutent après une réclamation, c'est la version qui coûte cher.

CE QUE LES SOUSCRIPTEURS DEMANDENT VRAIMENT

De plus en plus, un « oui » doit être prouvé, que ce soit à la proposition, au renouvellement ou après une réclamation :

- Captures d'écran des politiques d'authentification multifacteur et d'Accès conditionnel, et rapports d'inscription.
- Exports de la console EDR montrant la couverture, et le nom du fournisseur de surveillance 24/7.
- Configuration des sauvegardes (immutabilité, conservation, identifiants distincts) et preuve d'un test de restauration.
- Les résultats de leur propre balayage externe, qu'on vous demandera d'expliquer ou de corriger avant la mise en vigueur de la couverture.
- Des questionnaires complémentaires sur les rançongiciels, qui approfondissent les mêmes mesures.

Gardez un dossier de ces preuves, daté, avec votre proposition signée. Si vous présentez un jour une réclamation, c'est la première chose que votre avocat coordonnateur voudra voir.

Ce guide ne constitue pas un avis juridique ni un conseil en assurance. Faites réviser vos réponses par votre courtier avant de signer.

Nous révisons les propositions avec nos clients avant qu'ils les signent. Écrivez-nous.

Besoin d'un deuxième regard?

Parlez directement à l'expert qui dirigerait le mandat.

