Proposition

Assurance contre les cyber-risques

Renseignements de base sur l'entreprise

Veuillez inscrire les renseignements suivants concernant l'ensemble de l'entreprise ou du groupe (y compris toutes les filiales) qui présente une proposition d'assurance :

1. Nom de l'entreprise : _____
   Secteur d'industrie principal : _____
2. Adresse principale : _____
   Province : _____ Code postal : _____ Pays : _____
3. Description des activités commerciales : _____
4. Adresse du site Web : _____
5. Date de fondation (jj/mm/aaaa) : _____
6. Nombre d'employés : _____
7. Revenu brut des derniers 12 mois : _____ $
   Profit brut des derniers 12 mois : _____ $
   Revenus provenant des ventes aux États-Unis : _____ %
8. Veuillez préciser la ou les institutions financières que vous utilisez pour vos opérations bancaires commerciales :
   _____

Coordonnées du contact principal

Afin de nous permettre de fournir des informations sur le téléchargement de notre application de réponse aux incidents et l'envoi des alertes et mises à jour sur la gestion des risques, veuillez fournir les coordonnées de la personne la plus appropriée au sein de votre organisation pour recevoir ces mises à jour :

9. Nom de la personne contact : _____ Titre : _____
   Adresse électronique : _____ Numéro de téléphone : _____

Questions de base concernant les risques

10. Veuillez confirmer si l'authentification multifactorielle est toujours activée sur tous vos comptes de courriel pour l'accès à distance : OUI ☐ NON ☐
11. Effectuez-vous des sauvegardes hors ligne quotidiennes de toutes les données critiques? OUI ☐ NON ☐
12. Veuillez confirmer le nom de votre fournisseur de services gérés (le cas échéant) : _____
13. Une partie de votre infrastructure informatique est-elle sous-traitée à des fournisseurs de technologies tiers, y compris des fournisseurs de services d'application? OUI ☐ NON ☐
    Si vous avez répondu oui à la question ci-dessus, veuillez énumérer vos fournisseurs de technologies tiers principaux dans la section appropriée à la fin de ce formulaire de proposition (maximum de 10).

Incidents cybernétiques précédents

14. Veuillez cocher toutes les cases ci-dessous concernant tout incident cybernétique dont vous avez été victime au cours des trois dernières années (il n'est pas nécessaire de mentionner les événements qui ont été bloqués avec succès par des mesures de sécurité) :
    ☐ Attaque par déni de service ☐ Atteinte à la vie privée ☐ Cybercriminalité ☐ Cyberextorsion
    ☐ Infection par maliciel ☐ Perte de données ☐ Rançongiciel ☐ Violation d'adresse IP
    ☐ Autre (veuillez préciser) : _____

500-1400, place Blair Towers • Ottawa ON K1J 9B8 • 1-800-267-8864 • assurancevictor.ca

15. Si vous avez coché l'une des cases ci-dessus, le ou les incidents ont-ils eu une conséquence financière directe de plus de 10 000 $ sur votre entreprise? OUI ☐ NON ☐

    Dans l'affirmative, veuillez fournir des renseignements supplémentaires ci-dessous, incluant des détails sur l'impact financier et les mesures prises pour éviter que l'incident ne se reproduise :

    _____

    _____

    _____

Analyse des revenus

Veuillez répondre aux questions ci-dessous. Si les renseignements exacts ne sont pas disponibles, veuillez fournir l'estimation la plus juste possible et indiquer que vous avez adopté cette méthode.

16. Veuillez fournir les renseignements suivants pour vos cinq clients principaux :

Nom du client	Principaux services	Revenu annuel
		$
		$
		$
		$
		$

Ressources et infrastructure informatiques

17. Quelles ont été vos dépenses opérationnelles approximatives en matière de sécurité informatique au cours du dernier exercice financier (y compris les salaires, les licences annuelles, les frais de conseil, etc.) : _____ $

18. Quel a été le montant approximatif de vos dépenses d'investissement en matière de sécurité informatique au cours du dernier exercice financier (y compris le matériel, les coûts ponctuels des logiciels, etc.) : _____ $

19. Prévoyez-vous dépenser plus, autant ou moins au cours de l'exercice financier en cours? _____

20. Votre infrastructure informatique est-elle principalement exploitée et gérée à l'interne ou externalisée? _____

21. Combien d'employés à temps plein compte votre département informatique? _____

22. Combien de ces employés se consacrent à un rôle dans la sécurité informatique? _____

Gouvernance de la sécurité de l'information

23. Qui est responsable de la sécurité informatique dans votre organisation (par titre du poste)?

    _____

24. Depuis combien de temps cette personne occupe-t-elle ce poste au sein de votre entreprise? _____

25. Veuillez décrire le type, la nature et le volume des données stockées sur votre réseau, y compris une estimation approximative du volume total d'individus uniques sur lesquels vous détenez des données :

    _____

    _____

    _____

26. Veuillez décrire votre politique de conservation des données, en précisant la fréquence à laquelle vous éliminez les enregistrements qui ne sont plus nécessaires :

    _____

27. Veuillez décrire en détail votre politique de sauvegarde des données, notamment la fréquence des sauvegardes, la technologie utilisée, les types de sauvegardes, la méthode de stockage utilisée (en ligne ou hors ligne), la fréquence à laquelle vous testez les sauvegardes et la manière dont vous protégez vos sauvegardes :

28. Adhérez-vous à des normes internationales reconnues en matière de gouvernance de l'information?
OUI ☐ NON ☐

Dans l'affirmative, lesquelles : _____

Contrôles en matière de cybersécurité

29. Si votre organisation utilise le protocole RDP (protocole de bureau à distance) pour permettre l'accès à distance à votre réseau, veuillez décrire les mesures que vous avez mises en place pour le sécuriser :

30. Veuillez décrire le processus que vous avez mis en place pour la correction de tous les systèmes d'exploitation et toutes les applications :

31. Selon quelle fréquence procédez-vous à l'analyse de la vulnérabilité de votre périmètre réseau? _____

32. Selon quelle fréquence procédez-vous à des tests d'intrusion de votre architecture de réseau? _____

33. Veuillez fournir des informations concernant les fournisseurs tiers que vous utilisez pour effectuer des tests d'intrusion :

34. Veuillez cocher toutes les cases ci-dessous concernant les contrôles actuellement mis en place dans votre infrastructure informatique (y compris ceux qui sont fournis par un tiers). Si vous n'êtes pas certain(e) de ce que sont ces outils, veuillez consulter les explications à la dernière page du présent formulaire.

- ☐ Atténuation des attaques de déni de service distribué
- ☐ Balayage de vulnérabilité
- ☐ Chiffrement d'appareils mobiles
- ☐ Cryptage des bases de données
- ☐ DMARC
- ☐ Filtrage de contenu d'Internet
- ☐ Filtrage de noms de domaine (DNS)
- ☐ Filtrage des courriels
- ☐ Formation de sensibilisation des employés
- ☐ Gestion d'information et d'événements de sécurité
- ☐ Inventaire des actifs informatiques
- ☐ Pare-feu applicatif Web (WAF)
- ☐ Pare-feu de périmètre
- ☐ Plan d'intervention en cas d'incident
- ☐ Prévention des pertes de données
- ☐ Renseignements personnalisés de menaces
- ☐ Sécurité des terminaux
- ☐ Surveillance du réseau
- ☐ Système de détection d'intrusion
- ☐ Tests d'intrusion
- ☐ Utilisation d'une liste blanche des applications

35. Veuillez fournir le nom du fournisseur de logiciels ou de services que vous utilisez pour chacun des contrôles sélectionnés ci-dessus :

36. Veuillez énumérer ci-dessous vos fournisseurs de technologies tiers principaux (maximum de 10) :

Protection de données

En acceptant cette assurance, vous consentez à ce que CFC Underwriting utilise les renseignements qu'elle pourrait détenir à votre sujet dans le but d'offrir la couverture d'assurance, de traiter les réclamations, s'il y a lieu, et de traiter des renseignements personnels délicats sur vous lorsque nécessaire (p. ex., renseignements médicaux ou condamnations pénales). Cela signifie que nous pourrions devoir divulguer certains renseignements à des tiers intervenants dans l'offre de l'assurance, par exemple des assureurs, experts en sinistres tiers, services de détection et de prévention de la fraude, compagnies de réassurance et autorités de réglementation en assurance. CFC Underwriting pourrait également utiliser des éléments dépersonnalisés de vos données pour l'analyse des tendances de l'industrie et pour fournir des données d'étalonnage. Pour des informations complémentaires concernant leur politique de confidentialité, visitez le site www.cfcunderwriting.com/privacy (disponible uniquement en anglais pour le moment)**.**

Si lesdits renseignements personnels délicats concernent une autre personne que vous, vous devez obtenir le consentement explicite de cette personne autorisant la divulgation de ces renseignements à CFC Underwriting et leur utilisation de ceux-ci aux fins susmentionnées. Les renseignements fournis seront traités confidentiellement et en conformité avec les lois applicables en matière de protection des données. Vous avez le droit de demander une copie de vos renseignements (CFC Underwriting pourrait appliquer des frais minimes pour la produire) et la correction de tout renseignement inexact.

Important – Police d'assurance contre les cyber-risques, Déclaration de faits

En acceptant cette assurance, vous confirmez que les faits indiqués dans le formulaire de proposition sont véridiques. Ces déclarations, de même que tout renseignement que vous, ou toute personne agissant en votre nom, avez fourni avant que CFC Underwriting accepte de vous assurer, forment la base de votre police et en font partie intégrante. Si quelque renseignement que ce soit dans ces déclarations s'avère inexacte, CFC Underwriting sera en droit de considérer cette assurance comme nulle et non avenue. Vous devriez conserver la présente déclaration de faits et une copie du formulaire de proposition rempli dans vos dossiers.

Le proposant doit signer la présente proposition. La signature de cette proposition ne garantit pas l'assurance. En ce qui touche les risques aux États-Unis, veuillez noter que dans certains États, toute personne qui soumet, sciemment et avec l'intention de frauder une compagnie d'assurance ou toute autre personne, une proposition d'assurance contenant de faux renseignements ou qui dissimule l'intention de fournir des renseignements trompeurs sur des faits importants à cet égard, commet un acte frauduleux vis-à-vis de l'assurance, ce qui constitue un crime.

Le soussigné est un dirigeant, associé, administrateur, gestionnaire de risques ou employé autorisé du proposant et certifie qu'une vérification raisonnable a été effectuée pour obtenir les réponses ici fournies, réponses qu'il déclare véridiques, exactes et complètes à sa connaissance. Une telle vérification raisonnable comprend toutes les démarches nécessaires auprès de collègues dirigeants, associés, administrateurs, gestionnaires de risques ou employés pour vous permettre de répondre aux questions correctement.

Nom de la personne contact (caractères d'imprimerie)	Titre
Signature	Date (jj/mm/aaaa)

Les contrôles en matière de cybersécurité expliqués

Atténuation des attaques de déni de service distribué
Matériel informatique ou solutions informatique en nuage utilisés pour filtrer et bloquer le trafic malveillant associé à une attaque par déni de service distribué tout en permettant aux utilisateurs légitimes de continuer à accéder au site Web de l'entité ou à ses services en ligne.

Authentification à deux facteurs
Quand un utilisateur s'authentifie par deux moyens lorsqu'il ouvre une session à distance dans un système informatique ou un service en ligne. Ces deux moyens sont typiquement un mot de passe et un code généré par un dispositif de jeton physique ou un logiciel.

Balayage de vulnérabilité
Tests automatisés conçus pour sonder les systèmes ou les réseaux informatiques et déceler la présence de vulnérabilités connues qui permettraient à des auteurs de cybermenaces d'obtenir un accès à un système.

Chiffrement d'appareils mobiles
Le chiffrement implique de brouiller les données à l'aide de techniques cryptographiques afin qu'elles puissent être lues uniquement par une personne possédant une clé spécifique. Quand le chiffrement est activé, le disque dur d'un appareil est crypté lorsque l'appareil est verrouillé. Le code ou le mot de passe de l'utilisateur agit comme clé spécifique.

Cryptage des bases de données
Quand les données sensibles sont cryptées pendant qu'elles sont détenues dans les bases de données. Si cette mesure est mise en place correctement, elle peut empêcher des auteurs de cybermenaces de lire les données sensibles s'ils réussissent à accéder à la base de données.

DMARC
Un protocole Internet utilisé pour lutter contre l'usurpation d'adresse électronique, une technique utilisée par les pirates informatiques dans des campagnes d'hameçonnage.

Filtrage de contenu d'Internet
Le filtrage de certaines pages ou de certains services Web jugés comme potentiellement menaçant à la sécurité d'une organisation. Par exemple, des sites d'Internet reconnus comme malveillants sont typiquement bloqués à l'aide d'une forme de filtrage de contenu d'Internet.

Filtrage de noms de domaine (DNS)
Une technique précise pour bloquer l'accès à des adresses IP malveillantes reconnues par les utilisateurs de votre réseau.

Filtrage des courriels
Logiciel utilisé pour balayer et catégoriser les courriels entrants et sortants afin de filtrer les pourriels et autre contenu malveillant.

Formation de sensibilisation des employés
Des programmes de formation conçus pour accroître la sensibilisation des employés en matière de sécurité. Par exemple, les programmes peuvent être axés sur le moyen d'identifier des courriels d'hameçonnage potentiel.

Fournisseurs de services gérés
Une organisation tierce qui fournit des services informatiques, y compris des services au niveau des réseaux, de l'infrastructure, de la sécurité informatique, du soutien technique et de l'administration informatique.

Gestion d'information et d'événements de sécurité
Système utilisé pour cumuler, corréler et analyser la sécurité des réseaux et de l'information, y compris les messages, les journaux et les alertes générés par différentes solutions en matière de sécurité dans l'ensemble du réseau.

Inventaire des actifs informatiques
Une liste de tout le matériel et des appareils informatiques détenus, exploités ou gérés par une entité. De telles listes sont typiquement utilisées pour évaluer les données détenues et les mesures de sécurité mises en place dans tous les dispositifs.

Pare-feu applicatif Web (WAF)
Protège les serveurs Web et leurs applications d'une intrusion ou d'une utilisation malveillante en inspectant et en bloquant les demandes nuisibles et le trafic Internet malveillant.

Pare-feu de périmètre
Des solutions de matériel informatique utilisées pour contrôler et surveiller le trafic du réseau entre deux points selon des paramètres prédéfinis.

Plan d'intervention en cas d'incident
Des plans d'action pour faire face aux incidents cybernétiques afin d'aider à guider le processus décisionnel de l'organisation et revenir au fonctionnement normal le plus rapidement possible.

Prévention des pertes de données
Logiciel qui peut déterminer si les données sensibles sont extraites d'un réseau ou d'un système informatique.

Renseignements personnalisés de menaces
La collecte et l'analyse de données provenant de renseignement de sources ouvertes (OSINT) et de sources du Dark Web pour fournir aux organisations des renseignements relatifs aux menaces cybernétiques et aux auteurs de ces cybermenaces.

Sécurité des terminaux
Logiciel installé sur les ordinateurs individuels (terminaux) qui utilise l'analyse basée sur le comportement et la signature pour identifier et arrêter les infections par maliciel.

Surveillance du réseau
Un système qui utilise un logiciel, un matériel informatique ou une combinaison des deux et qui surveille constamment les problèmes de performance et sécurité du réseau d'une organisation.

Système de détection d'intrusion
Une solution en matière de sécurité qui surveille l'activité sur les systèmes ou réseaux informatiques et génère des alertes quand elle détecte des signes d'un danger émanant d'auteurs de cybermenaces.

Tests d'intrusion
La simulation autorisée d'attaques contre une organisation pour mettre à l'épreuve ses défenses en matière de cybersécurité. Cette technique s'appelle aussi piratage contrôlé ou méthode de l'équipe rouge.

Utilisation d'une liste blanche des applications
Une solution de sécurité qui permet aux organisations de préciser quels logiciels sont autorisés à fonctionner dans leurs systèmes afin de prévenir le fonctionnement de tout processus ou de toute application non-listé sur la liste blanche.