Proposition

Assurance contre les cyber-risques

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 et qui partage l'interconnectivité du réseau.

Tous les termes définis sont en gras et surlignés en **orange** et peuvent être trouvés dans le glossaire de contrôles en matière de cybersécurité à la fin de ce formulaire de proposition.

Renseignements de base sur l'entreprise

1. Nom de l'entreprise (nom légal et nom commercial si applicable) : _____

   _____

   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 : _____ $ Revenus provenant des ventes aux États-Unis : _____ %

   Profit brut des derniers 12 mois : _____ $

8. Veuillez préciser la ou les institution(s) financière(s) que vous utilisez pour vos opérations bancaires commerciales :

   _____

Coordonnées du contact principal

Veuillez fournir les coordonnées de la personne au sein de votre organisation qui est principalement responsable de la sécurité informatique. Ces coordonnées seront utilisées pour fournir des informations sur le téléchargement de notre application de réponse aux incidents et pour recevoir des alertes et des mises à jour sur la gestion des risques.

9. Nom de la personne contact : _____ Titre : _____

   Adresse électronique : _____ Numéro de téléphone : _____

Incidents cybernétiques antérieurs

10. 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 ☐ Cyberextorsion
    ☐ Infection par maliciel ☐ Perte de données ☐ Rançongiciel
    ☐ Violation de l'adresse IP ☐ Vol de fonds
    ☐ Autre (veuillez préciser) : _____

11. Si vous avez coché l'une des cases ci-dessus, le(s) incident(s) a-t-il(ont-ils) eu un impact financier direct de plus de 10 000 $? 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 :

    _____

    _____

    _____

500-1400, place Blair Towers • Ottawa ON K1J 9B8 • 1-800-267-6684 • assurancevictor.ca
© 2023 Gestionnaires d'assurance Victor inc.

Analyse des revenus

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

Nom du client	Principaux services	Revenus annuels provenant de ce client
		$
		$
		$
		$
		$

Ressources et infrastructure informatiques

13. Veuillez confirmer le nom de votre **fournisseur de services gérés** (le cas échéant) : _____

14. Quel est le nombre approximatif de serveurs sur votre réseau? _____

15. Quel est le nombre approximatif d'ordinateurs de bureau et d'ordinateurs portables sur votre réseau? _____

16. Quel est votre budget informatique annuel? _____ $

17. Quel pourcentage approximatif de votre budget informatique est consacré à la sécurité informatique? _____ %

18. Une partie de votre infrastructure informatique est-elle sous-traitée à des fournisseurs de technologie tiers, y compris des fournisseurs de services d'application? OUI ☐ NON ☐

    Dans l'affirmative, veuillez énumérer ci-dessous vos fournisseurs de technologies tiers principaux (maximum de 10), y compris un bref résumé des services technologiques qu'ils vous fournissent :

    _____

    _____

    _____

    _____

    _____

Stockage et gestion des données

19. Veuillez indiquer le nombre approximatif d'individus uniques auprès desquels vous recueillez, stockez et/ou traitez les informations personnelles identifiables, que ce soit sur vos propres systèmes ou avec des tierces parties :

Type de données	Nombre d'individus uniques
Données sensibles (par exemple, dossiers médicaux, détails du passeport, numéros de sécurité sociale, etc.) :	
Données non sensibles (par exemple, les noms complets, les adresses, les adresses électroniques, etc.) :	

20. Veuillez décrire votre approche de la protection des informations sensibles et confidentielles (par exemple, contrôles d'accès, cryptage, segmentation du réseau, etc.) :

    _____

    _____

21. Veuillez fournir des détails sur la fréquence à laquelle vous éliminez les enregistrements qui ne sont plus nécessaires :

    _____

    _____

22. Veuillez fournir des détails sur la manière dont vous stockez vos sauvegardes de données critiques (par exemple, des sauvegardes en ligne stockées sur l'environnement réel de votre organisation, des sauvegardes hors ligne

© 2023 Gestionnaires d'assurance Victor inc.

stockées sur un dispositif de stockage amovible entièrement déconnecté et inaccessible depuis l'environnement réel, des sauvegardes stockées chez un fournisseur de stockage en nuage en ligne, etc.) :

23. Veuillez décrire des détails sur la fréquence des sauvegardes, y compris la fréquence des sauvegardes complètes du système et la fréquence des sauvegardes incrémentielles/différentielles des données critiques :

24. Veuillez fournir des détails sur la manière dont vous sécurisez vos sauvegardes (par exemple, les sauvegardes sont déconnectées et inaccessibles depuis l'environnement réel, une **authentification multifactorielle** est requise pour l'accès aux sauvegardes dans le nuage, etc.) :

25. Veuillez fournir des détails sur la façon dont vous testez vos sauvegardes, y compris des détails sur la fréquence à laquelle vous testez la restauration complète et la récupération des configurations de serveurs clés et des données à partir des sauvegardes :

26. Veuillez fournir des détails sur le nombre de copies de sauvegarde que vous faites, y compris des détails sur la façon dont vous empêchez que des copies de sauvegarde distinctes soient affectées par le même événement (le cas échéant) :

Sécurité des points d'extrémité

27. Quel outil de **protection des points d'extrémité** utilisez-vous sur votre réseau? _____

    Veuillez indiquer le nom du vendeur et l'outil utilisé :

28. Utilisez-vous un outil de **détection et réponse aux points d'extrémité (EDR)** sur votre réseau?OUI ☐ NON ☐

    Dans l'affirmative, quel outil utilisez-vous : _____

29. Veuillez donner un aperçu de la manière dont votre outil EDR est surveillé et géré (par exemple, par une équipe informatique interne ou par une tierce partie) :

30. L'outil EDR est-il déployé sur tous les points d'extrémité de votre réseau? OUI ☐ NON ☐

    Dans la négative, quel est le pourcentage des points d'extrémité pour lesquels le système EDR n'est pas déployé et pourquoi n'est-il pas déployé sur ces points d'extrémité :

Sécurité du périmètre

31. Avez-vous déployé des **pares-feux de nouvelle génération** à tous les points d'entrée et de sortie du réseau? OUI ☐ NON ☐

32. Selon quelle fréquence procédez-vous au **balayage de vulnérabilité** de votre périmètre réseau? _____

© 2023 Gestionnaires d'assurance Victor inc.

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

34. Veuillez fournir des informations concernant les fournisseurs tiers que vous utilisez pour effectuer des tests d'intrusion (le cas échéant) :

_____

_____

35. Veuillez confirmer si l'**authentification multifactorielle** est requise pour **tous les accès à distance à votre réseau** : OUI ☐ NON ☐

36. Si vous utilisez une autre méthode pour sécuriser l'accès à distance à votre réseau, comme l'authentification par certificat pour les appareils, veuillez fournir des détails :

_____

_____

37. Veuillez confirmer si l'**authentification multifactorielle** est requise pour accéder à **toutes les ressources en nuage contenant des informations sensibles ou confidentielles** : OUI ☐ NON ☐

Sécurité du périmètre courriel

38. Veuillez confirmer que l'**authentification multifactorielle** est activée pour l'accès à distance à **tous les comptes de messagerie de l'entreprise** : OUI ☐ NON ☐

39. Simulez-vous des attaques d'hameçonnage pour tester les employés au moins une fois par an? OUI ☐ NON ☐

40. Utilisez-vous un logiciel de **filtrage des courriels** pour analyser tous les courriels entrants et sortants afin de filtrer les pourriels et les contenus malveillants? OUI ☐ NON ☐

    Dans l'affirmative, veuillez indiquer le nom du fournisseur et le produit utilisé pour le filtrage des courriels :

    _____

41. Si vous êtes un utilisateur d'Office 365, veuillez fournir votre Microsoft Secure Score (les administrateurs peuvent trouver le score en utilisant le lien suivant https://security.microsoft.com/securescore) :

    _____

Sécurité du réseau

42. Veuillez fournir des détails sur la manière dont vous protégez les comptes d'utilisateurs privilégiés (par exemple, en utilisant des solutions de gestion des accès privilégiés, en limitant les comptes d'utilisateurs privilégiés à des appareils spécifiques, en surveillant de manière accrue les comptes pour détecter toute utilisation anormale, en activant l'authentification multifactorielle pour l'accès à distance, etc.) :

    _____

    _____

43. Les utilisateurs non informatiques ont-ils des droits d'administrateur local sur leurs ordinateurs portables/de bureau? OUI ☐ NON ☐

44. Utilisez-vous une solution de **surveillance du réseau** pour alerter votre organisation en cas d'activité suspecte ou de comportement malveillant sur votre réseau? OUI ☐ NON ☐

    Dans l'affirmative, veuillez indiquer le nom du fournisseur et le produit utilisé pour la surveillance du réseau :

    _____

45. Veuillez indiquer si vous disposez d'un **centre des opérations de sécurité (SOC)** chargé de la surveillance et de la détection des événements, de la gestion des vulnérabilités et de la réponse aux incidents. Veuillez inclure des détails sur les heures de fonctionnement et préciser s'il s'agit d'une fonction interne ou externalisée à une tierce partie :

    _____

    _____

© 2023 Gestionnaires d'assurance Victor inc.

46. Utilisez-vous un logiciel en fin de vie (EOL/EOS)? OUI ☐ NON ☐

Dans l'affirmative, veuillez fournir des détails sur la nature du logiciel en fin de vie (EOL/EOS), la manière dont il est utilisé, s'il est séparé du reste du réseau et si oui, comment il est séparé :

47. Veuillez décrire votre processus de gestion des correctifs et la manière dont vous vous assurez que tous les correctifs critiques sont appliqués en temps opportun, y compris un calendrier de mise en œuvre des correctifs pour les vulnérabilités zero-day après leur publication par le fournisseur :

48. Veuillez fournir des détails sur les changements majeurs que vous avez prévus pour votre infrastructure informatique au cours des 12 prochains mois (le cas échéant) :

Contrôles supplémentaires

49. Veuillez confirmer qu'**avant** toute modification des détails du compte d'une tierce partie, vous obtenez l'autorisation de ce dernier par une méthode d'authentification différente de la méthode initiale utilisée pour demander la modification : OUI ☐ NON ☐

50. Veuillez confirmer qu'**avant** de transférer des fonds vers un compte sur lequel vous n'avez jamais versé d'argent, vous obtenez l'autorisation du destinataire des fonds par une méthode d'authentification différente de la méthode initiale utilisée pour demander le transfert : OUI ☐ NON ☐

51. Fournissez-vous une formation sur les escroqueries par hameçonnage/ingénierie sociale à tous les employés impliqués dans le transfert de fonds au nom de votre organisation, au moins une fois par an? OUI ☐ NON ☐

52. 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 sûr 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
- ☐ DMARC
- ☐ Filtrage de noms de domaine (DNS)
- ☐ Gestion d'information et d'événements de sécurité
- ☐ Pares-feux de périmètre
- ☐ Plan d'intervention en cas d'incident
- ☐ Renseignements personnalisés de menaces
- ☐ Tests d'intrusion
- ☐ Cryptage des bases de données
- ☐ Filtrage de contenu d'Internet
- ☐ Formation de sensibilisation des employés
- ☐ Inventaire des actifs informatiques
- ☐ Pares-feux pour application Web (WAF)
- ☐ Prévention des pertes de données
- ☐ Réseau privé virtuel (VPN)
- ☐ Utilisation d'une liste blanche des applications

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

Limites et franchises

54. Veuillez indiquer les limites et les franchises pour lesquelles vous souhaitez obtenir des soumissions :

(a) Cyber et vie privée

Limite	Franchise
☐ 250 000 $	☐ 2 500 $
☐ 500 000 $	☐ 5 000 $
☐ 1 000 000 $	☐ 10 000 $
☐ 2 000 000 $	☐ 15 000 $
☐ 3 000 000 $	☐ 20 000 $
Autre (veuillez préciser) :	Autre (veuillez préciser) :

© 2023 Gestionnaires d'assurance Victor inc.

(b) Crime cybernétique

Limite	Franchise
☐ 50 000 $	☐ 2 500 $
☐ 75 000 $	☐ 5 000 $
☐ 100 000 $	☐ 10 000 $
☐ 150 000 $	☐ 15 000 $
☐ 250 000 $	☐ 20 000 $
Autre (veuillez préciser) :	Autre (veuillez préciser) :

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)

© 2023 Gestionnaires d'assurance Victor inc.

Les contrôles en matière de cybersécurité expliqués

Atténuation des attaques de déni de service distribué
Matériel informatique ou solutions axées sur l'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 multifactorielle
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.

Centre des opérations de sécurité (SOC)
Une installation qui abrite une équipe de sécurité de l'information chargée de surveiller et d'analyser en permanence la posture de sécurité d'une organisation. L'objectif de l'équipe SOC est de détecter, d'analyser et de répondre aux incidents de cybersécurité en utilisant une combinaison de solutions technologiques et un ensemble de processus solides. Les SOC peuvent être internes et gérés par l'organisation elle-même ou externalisés à une tierce partie.

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.

Détection et réponse aux points d'extrémité (EDR)
Un outil logiciel qui fonctionne en surveillant et en collectant des données à partir de points finaux et en enregistrant les informations dans une base de données centrale où se déroulent des analyses, des détections, des enquêtes, des rapports et des alertes supplémentaires.

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 aux 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.

Pares-feux de nouvelle génération
Solutions logicielles ou matérielles qui combinent la technologie traditionnelle des pares-feux avec des fonctionnalités supplémentaires, telles que l'inspection du trafic crypté, les systèmes de prévention des intrusions et les antivirus.

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

Pares-feux pour application Web (WAF)
Protègent 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.

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.

Protection des points d'extrémité
Logiciel installé sur des ordinateurs individuels (points d'extrémité) qui utilise l'analyse du comportement et des signatures pour identifier et arrêter les infections par des logiciels malveillants.

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 cybermenaces pertinents.

Réseau privé virtuel (VPN)
Un VPN est une connexion cryptée sur l'internet entre un appareil et un réseau. La connexion cryptée permet de garantir que les données sensibles sont transmises en toute sécurité. Il est le plus souvent utilisé pour fournir une connexion à distance sécurisée au réseau d'une organisation.

Surveillance de réseau
Un système qui utilise le logiciel, le 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 vos 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 peuvent être utilisés dans leurs systèmes afin de prévenir le fonctionnement de tout processus ou de toute application non-listé sur la liste blanche.

© 2023 Gestionnaires d'assurance Victor inc.