Cyber

Entreprise privée

Formulaire de demande
Canada

Entreprise Privée

Formulaire de demande d'assurance en matière de cybersécurité

CAN

Ce formulaire de demande est destiné aux entreprises avec un revenu de moins de 50 millions de dollars et désirant une limite d'assurance en matière de cybersécurité de 5 millions de dollars et moins. Pour obtenir d'autres renseignements sur la couverture offerte ou de l'aide pour remplir ce formulaire, veuillez consulter notre site Web au: **www.cfcunderwriting.com/cyber**

Renseignements de base sur l'entreprise

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

Nom de l'entreprise:

Principal secteur industriel:

Adresse principale (adresse, province, code postal, pays):

Descriptions des activités commerciales :

Adresse du site Web:

Date de fondation (JJ/MM/AAAA):

Revenu du dernier exercice complété: $

Revenu provenant des ventes aux États-Unis (%) :

Renseignements sur la personne-ressource principale

Veuillez fournir les renseignements sur la personne-ressource principale pour la police d'assurance :

Nom du contact:

Fonction:

Adresse électronique:

Numéro de téléphone:

Couverture requise

Veuillez indiquer pour quelles options de limite vous aimeriez recevoir une soumission (si la couverture n'est pas requise dans un domaine en particulier, veuillez ne rien inscrire)

Frais d'intervention en cas d'incident:	☐ $250k	☐ $500k	☐ $1m	☐ $2m	☐ $5m	☐ Autre $
Cyber-responsabilité et responsabilité relative aux atteintes à la vie privée:	☐ $250k	☐ $500k	☐ $1m	☐ $2m	☐ $5m	☐ Autre $
Dommages aux systèmes et pertes d'exploitation:	☐ $250k	☐ $500k	☐ $1m	☐ $2m	☐ $5m	☐ Autre $
Crime cybernétique:	☐ $100k	☐ $250k	☐ $1m	☐ Other $		

©1999-2019 CFC Underwriting Ltd, tous droits réservés

Cyberincidents précédents

Veuillez cocher toutes les cases ci-dessous concernant tout cyberincident dont vous avez été victime au cours des trois dernières années (ne mentionnez pas les événements qui ont été bloqués avec succès par les mesures de sécurité):

☐ Crime cybernétique ☐ Extorsion cybernétique ☐ Perte de données ☐ Attaque par déni de service ☐ Violation d'adresse IP

☐ Infection par maliciel ☐ Atteinte à la vie privée ☐ Logiciel rançonneur ☐ Autre (veuillez préciser)

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 k $ sur votre entreprise?

☐ Oui ☐ Non

Si oui, veuillez fournir des renseignements supplémentaires ci-dessous, y compris les détails de la conséquence financière et des mesures prises pour empêcher cet incident de se reproduire :

Avis important

En signant ce formulaire, vous confirmez que les renseignements fournis sont exacts et complets et que vous avez pris toutes les mesures raisonnables pour vous en assurer en vous adressant aux personnes concernées au sein de votre entreprise. CFC Underwriting utilisera ces renseignements uniquement pour fournir des services d'assurance et pour ce faire, elle pourrait partager vos données avec des tiers.
Nous pourrions également utiliser des éléments dépersonnalisés de vos données pour l'analyse des tendances de l'industrie et pour fournir des données d'étalonnage. Pour plus de détails sur notre politique de confidentialité, veuillez visiter ***www.cfcunderwriting.com/privacy***

Nom du contact: Fonction :

Signature: Date (JJ/MM/AAAA):

©1999-2019 CFC Underwriting Ltd, tous droits réservés

Entreprise Privée

Formulaire supplémentaire de demande d'assurance en matière de cybersécurité

CAN

Ce formulaire supplémentaire et optionnel de demande nous aide à obtenir une vue d'ensemble plus complète de votre entreprise et de ses contrôles de sécurité. En remplissant cette demande supplémentaire d'information, vous serez admissible à un rabais de 25 % sur votre soumission. Pour obtenir d'autres renseignements sur la couverture offerte ou de l'aide pour remplir ce formulaire, veuillez consulter notre site Web au: ***www.cfcunderwriting.com/cyber***

Ressources et infrastructure informatiques

Veuillez répondre aux questions ci-dessous. Si les renseignements exacts ne sont pas disponibles, veuillez fournir l'estimation qui s'en rapproche le plus et indiquer que vous avez adopté cette méthode :

Nom de l'entreprise/Numéro de référence CFC :	
À quel montant environ s'élevaient vos dépenses opérationnelles pour la sécurité informatique au cours du dernier exercice financier (y compris les salaires, les licences annuelles, les frais de consultation, etc.):	
À quel montant environ s'élevaient vos dépenses en capital pour la sécurité informatique au cours du dernier exercice financier (y compris le matériel informatique, les coûts ponctuels de logiciels, etc.):	
Planifiez-vous dépenser plus, moins ou la même somme au cours de l'exercice financier en cours?	
Votre infrastructure informatique est-elle principalement exploitée et gérée en interne ou par sous-traitance?	
S'il s'agit d'une sous-traitance, à qui est-elle confiée?	
Combien d'employés à temps plein comptez-vous dans votre service informatique?	
Combien de ces employés se consacrent à un rôle en sécurité informatique?	

Gouvernance de la sécurité de l'information

Qui est responsable de la sécurité informatique dans votre organisation (par titre du poste)?	
Depuis combien de temps cette personne occupe-t-elle ce poste au sein de votre entreprise?	

Adhérez-vous à des normes internationales reconnues en matière de gouvernance de l'information (si oui, lesquelles):

Fournisseurs de services infonuagiques

Veuillez cocher toutes les cases ci-dessous concernant les entreprises ou les services que vous utilisés pour stocker les données sensibles ou vous fournir des services commerciaux essentiels:

☐ Adobe	☐ Amazon Web Services	☐ Dropbox	☐ Google Cloud
☐ IBM	☐ Microsoft 365	☐ Microsoft Azure	☐ Oracle Cloud
☐ Rackspace	☐ Salesforce	☐ SAP	☐ Workday

©1999-2019 CFC Underwriting Ltd, tous droits réservés

Entreprise Privée

Formulaire supplémentaire de demande d'assurance en matière de cybersécurité

Contrôles en matière de cybersécurité

Veuillez cocher toutes les cases ci-dessous concernant les contrôles actuellement mis en place dans votre infrastructure informatique (y compris ceux fournis par une tierce partie). Si vous n'êtes pas sûr de ce que sont ces outils, veuillez consulter les explications à la dernière page de ce document:

☐ Sécurité supérieure de point d'extrémité	☐ Application d'établissement de liste blanche	☐ Inventaire des actifs	☐ Information personnalisée relative aux menaces Web
☐ Cryptage des données	☐ Prévention des pertes de données	☐ Atténuation des attaques par DDOS	☐ DMARC
☐ Filtrage basé sur le DNS	☐ Formation de sensibilisation des employés	☐ Plan d'intervention en cas d'incident	☐ Système de détection des intrusions
☐ Cryptage des appareils mobiles	☐ Essais de pénétration	☐ Pare-feu périmétrique	☐ Gestion de la sécurité de l'information et des événements
☐ Authentification à deux facteurs	☐ Analyses de vulnérabilité	☐ Pare-feu pour application Web	☐ Filtrage de contenu Web

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

Avis important

En signant ce formulaire, vous confirmez que les renseignements fournis sont exacts et complets et que vous avez pris toutes les mesures raisonnables pour vous en assurer en vous adressant aux personnes concernées au sein de votre entreprise. CFC Underwriting utilisera ces renseignements uniquement pour fournir des services d'assurance et pour ce faire, elle pourrait partager vos données avec des tiers.
Nous pourrions également utiliser des éléments dépersonnalisés de vos données pour l'analyse des tendances de l'industrie et pour fournir des données d'étalonnage. Pour plus de détails sur notre politique de confidentialité, veuillez visiter ***www.cfcunderwriting.com/privacy***

Nom du contact: Fonction :

Signature: Date (JJ/MM/AAAA):

©1999-2019 CFC Underwriting Ltd, tous droits réservés

Les contrôles en matière de cybersécurité expliqués

Sécurité supérieure de point d'extrémité

Logiciel installé sur les ordinateurs individuels (points d'extrémité) qui utilise l'analyse basée sur le comportement et la signature pour identifier et stopper les infections par maliciel.

Application d'établissement de liste blanche

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 qui ne figurent pas sur la liste blanche.

Inventaire des actifs

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 stockées et les mesures de sécurité mises en place dans tous les dispositifs.

Information personnalisée relative aux menaces web

La collecte et l'analyse de données provenant de renseignement de sources ouvertes (OSINT) et de sources du Web invisible pour fournir aux organisations des renseignements relatifs aux menaces Web et aux acteurs hostiles qui les concernent.

Cryptage des données

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

Prévention Des Pertes De Données

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

Atténuation des attaques par DDoS

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

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 basé sur le DNS

Une technique précise pour bloquer l'accès à des adresses IP malveillantes reconnues aux utilisateurs de votre réseau.

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.

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 mode de fonctionnement normal le plus rapidement possible.

Système de détection des intrusions

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'acteurs hostiles.

Cryptage des appareils mobiles

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

Essais de pénétration

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.

Pare-feu périmétrique

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

Gestion de la sécurité de l'information et des événements

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.

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.

Analyses de vulnérabilité

Tests automatisés conçus pour sonder les systèmes ou les réseaux informatiques pour déceler la présence de vulnérabilités connues qui permettraient à des acteurs hostiles d'obtenir un accès à un système.

Pare-feu pour application Web

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.

Filtrage de contenu Web

Le filtrage de certaines pages ou de certains services Web jugés comme une menace potentielle à la sécurité d'une organisation. Par exemple, des sites Web malveillants connus sont typiquement bloqués à l'aide d'une certaine forme de filtrage de contenu Web.

©1999-2019 CFC Underwriting Ltd, tous droits réservés