CyberPrep de CNA

Une approche en trois axes pour se préparer en matière de cybersécurité

La cybercriminalité poursuit ses méfaits sans relâche et est de plus en plus pointue, fréquente et grave. Elle constitue même l'une des principales préoccupations des entreprises à l'échelle mondiale, selon le rapport sur les risques mondiaux 2021 du Forum économique mondial (en anglais seulement). Cyberprep de CNA est un programme proactif sur les cyberrisques mis en place par l'équipe du contrôle des risques et les souscripteurs en cyberassurance de CNA, en collaboration avec d'éminents spécialistes de la cybersécurité. Il s'appuie sur près de deux décennies d'expertise en cyberassurance et est conçu pour aider les titulaires de police d'assurance des cyberrisques de CNA à identifier les cybermenaces, à les atténuer et à réagir en conséquence.

À propos de Cyberprep de CNA

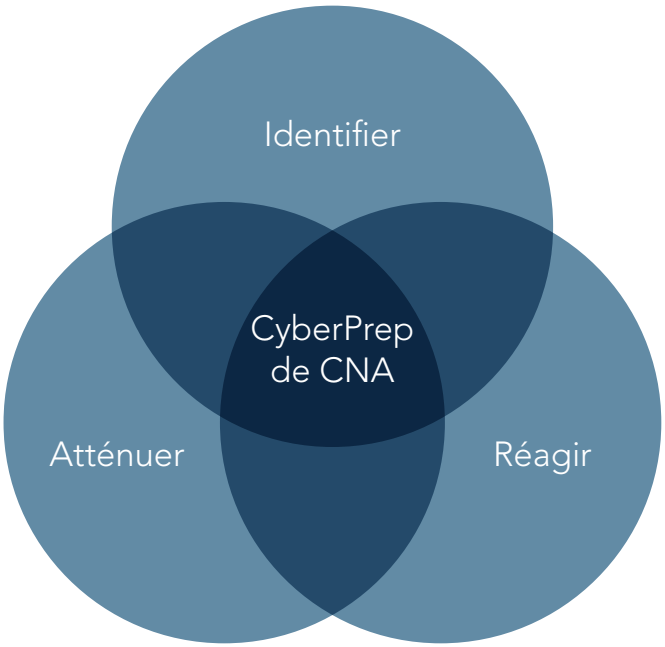
La présente brochure fournit aux assurés des informations générales sur des fournisseurs et des services. Les assurés qui souhaitent en savoir plus ou déterminer les services qui pourraient convenir à leur entreprise doivent communiquer avec leur courtier et leur souscripteur en cyberrisques de CNA.

Les rapports ainsi que les recommandations des fournisseurs dans le cadre du programme Cyberprep (autres que les services fournis par l'équipe du contrôle des risques de CNA) ne seront pas communiqués à CNA, à moins que l'assuré et son courtier ne décident de les partager.

L'utilisation des termes « partenariat » ou « partenaire » ne doit pas être interprétée comme représentant un partenariat liant juridiquement les parties.

CyberPrep de CNA

CyberPrep de CNA est offert à tous les titulaires de police d'assurance des cyberrisques de CNA et leur fournit un réseau de professionnels en cybersécurité ainsi que des services pour identifier efficacement les cyberrisques, les atténuer et réagir en cas de brèche de sécurité informatique. CyberPrep de CNA s'inspire de cadres à la pointe de l'industrie en matière de cybersécurité pour établir les normes, les lignes directrices et les meilleures pratiques à adopter, notamment sur celui du National Institute of Standards and Technology (NIST) des États-Unis, et s'appuie sur des partenariats solides avec des spécialistes en cybersécurité hautement réputés.



Identifier

Identifier les dispositifs de cybersécurité actuels : un groupe de fournisseurs et de services sélectionnés aide les assurés à identifier les forces et les faiblesses de leurs dispositifs de cybersécurité, et leur formule également des recommandations pour mettre en place des mesures de cybersécurité supplémentaires.

Atténuer

Atténuer les risques éventuels en matière de cybersécurité : d'autres fournisseurs et services mettent en œuvre les recommandations en matière de cybersécurité pour aider les assurés à améliorer leurs dispositifs de cybersécurité et atténuer les cyberrisques éventuels. Elles comprennent une protection antivirus nouvelle génération, la planification et la mise à l'essai de réponses aux cyberincidents, l'élaboration et la mise à l'essai de politiques et de procédures d'intervention en cas de cyberincident, la gestion des mots de passe, la formation des membres du personnel et l'authentification multifacteur.

Réagir

Réagir face à un cyberincident : les incidents liés à la sécurité sont souvent une source de stress important. Les fournisseurs de CNA spécialisés dans les interventions en cas de cyberincident ont des connaissances approfondies des étapes essentielles pour atténuer les conséquences d'un cyberincident et fournir de l'aide le cas échéant. Parmi les fournisseurs se trouvent des avocats spécialisés en brèches de sécurité informatique et en droit au domaine privé, des cabinets d'expertise judiciaire et spécialisés dans les mesures correctives, des fournisseurs de notification et de surveillance du crédit, ainsi que des sociétés de relations publiques.

Il est conseillé aux assurés de consulter leur courtier et leur souscripteur en cyberrisques de CNA pour en savoir plus sur chacun des services présentés dans la présente brochure.

Identifier

L'**identification** des dispositifs de cybersécurité est un point de départ essentiel du processus Cyberprep de CNA. Les services comprennent des analyses détaillées effectuées par un réseau de spécialistes en cybersécurité, des rapports fournissant un aperçu des dispositifs de cybersécurité des titulaires de police d'assurance et de nombreuses recommandations pour les améliorer. Les assurés en cyberrisques de CNA peuvent choisir des services de tarification préférentielle payants et des options à valeur ajoutée, qui font partie de leur police d'assurance des cyberrisques.

Services à valeur ajoutée

Analyse des lacunes en matière de contrôle des risques de CNA

L'analyse des lacunes porte sur les renseignements que fournissent les assurés au sujet de leurs programmes de sécurité de l'information. CNA propose une évaluation personnalisée conçue pour optimiser la confidentialité de l'information et réduire les vulnérabilités pouvant mener à une cyberattaque.

L'analyse des lacunes en matière de contrôle des risques de CNA :

- évalue les contrôles par rapport aux meilleures pratiques courantes du secteur;
- fournit une estimation des coûts liés à une brèche de sécurité informatique;
- identifie les conséquences attendues des efforts de prévention et d'atténuation des sinistres;
- formule des recommandations qui pourraient potentiellement réduire la fréquence ou la gravité des sinistres pour les risques identifiés comme à forte incidence.

Auto-analyse de la sécurité de l'information et de la cyberinfrastructure

Cet outil d'évaluation se base sur le cadre en matière de cybersécurité (identification, protection, détection, réaction et récupération) ainsi que sur les lignes directrices relatives à la sécurité de l'information des petites entreprises du National Institute of Standards and Technology (NIST) des États-Unis. Les résultats de l'évaluation permettent d'identifier les lacunes en matière de contrôle de la sécurité de l'information et de créer une base de référence afin d'évaluer les conséquences éventuelles des efforts de prévention et d'atténuation des sinistres.

Services à valeur ajoutée

CyberArk – Évaluation de la sécurité des accès à privilèges

L'évaluation de la sécurité des accès à privilèges de CyberArk aborde systématiquement les risques liés à la sécurité des accès à privilèges des entreprises et recommande la prise de mesures qui peuvent améliorer au maximum l'ensemble de leurs dispositifs de sécurité des accès à privilèges. Les analyses se basent sur sept facteurs essentiels tels que la protection contre les comptes de prise de contrôle irréversible du réseau et la sécurisation des informations d'identification des applications. Une cote de risque personnalisée permet à une entreprise de comparer son degré de sécurité des accès à privilèges à celui de paires en utilisant un groupe de référence défini en fonction du secteur d'activité, du nombre d'employés, du chiffre d'affaires annuel et de la région. Cette analyse comparative détaillée prodigue également des conseils en matière de mesures correctives.

Une fois l'évaluation terminée, l'assuré reçoit un rapport détaillé comprenant les résultats ainsi que des recommandations.

Un représentant de CyberArk est également disponible pour discuter du rapport avec l'assuré. *CNA ne reçoit pas le rapport d'évaluation de CyberArk à moins que l'assuré ne choisisse de le partager.*

Services de tarification préférentielle

Analyses de vulnérabilité externes

Une analyse de vulnérabilité externe recherche et identifie les vulnérabilités d'un réseau ou d'un site Web susceptibles d'être exploitées par un attaquant externe et recommande des mesures pour aider à les corriger. Le réseau Cyberprep de CNA comprend des fournisseurs qui peuvent effectuer des analyses de vulnérabilité externes.

Test d'intrusion

Un test d'intrusion simule une attaque sur votre réseau et sur vos applications afin de déterminer les vulnérabilités et de tenter de les exploiter. À l'issue du test est fourni un rapport comprenant des recommandations sur les mesures à prendre pour corriger les vulnérabilités identifiées. Le réseau Cyberprep de CNA comprend plusieurs fournisseurs de tests d'intrusion auxquels les assurés peuvent faire appel.

Évaluations des risques

CNA a établi des relations avec plusieurs fournisseurs qui proposent des évaluations des risques de différentes sortes qui permettent d'identifier les vulnérabilités au sein de l'environnement cybernétique et des technologies de l'information d'une entreprise.

Il est conseillé aux assurés de consulter leur courtier et leur souscripteur en cyberrisques de CNA pour en savoir plus sur chacun des services présentés dans la présente brochure.

Atténuer

Les assurés, en collaboration avec leur courtier, l'équipe du contrôle des risques et les souscripteurs en cyberrisques de CNA, appliquent les recommandations pour atténuer les cyberrisques et améliorer leurs dispositifs de cybersécurité. Les recommandations peuvent porter sur l'appel aux fournisseurs suivants, soit par l'entremise d'un service de tarification préférentielle payant, soit par celle d'options à valeur ajoutée incluses dans la police d'assurance des cyberrisques de CNA.

Services à valeur ajoutée

Portail Web eRiskHub® de CNA

CNA donne aux titulaires de police d'assurance des cyberrisques un accès au service en ligne eRiskHub®, qui fournit des outils et des ressources pour aider la clientèle à comprendre les cyberrisques, à réagir efficacement face aux brèches de sécurité informatique et à atténuer leurs conséquences sur les entreprises. De conseils de prévention à des recommandations pour réagir aux risques, eRiskHub® vous aidera à faire face à n'importe quelle situation liée aux cyberrisques.

Le portail eRiskHub® fournit des renseignements actualisés sur les cyberrisques et d'autres outils très utiles, notamment :

- des feuilles de route en cas d'incident;
- des actualités;
- des centres d'apprentissage;
- des outils pour les gestionnaires de risques;
- des ressources en ligne sur les risques.

Modules de formation informatisée

Grâce à sa relation avec Cofense, CNA peut offrir aux assurés en cyberrisques plus de 20 modules de formation informatisée sur le thème des cyberrisques, notamment sur le piratage psychologique, l'hameçonnage, la gestion des brèches de sécurité informatique et d'autres sujets pertinents. Remarque : Les modules de formation informatisée exigent un système de gestion de l'apprentissage (SGA). Veuillez contacter votre courtier ou votre souscripteur en cyberassurance pour en savoir plus sur ces services et sur l'achat d'un SGA à tarif préférentiel si nécessaire.

Consultation d'un avocat spécialisé en brèches de sécurité information approuvé par CNA

Chaque membre du groupe d'avocats spécialisés en brèches de sécurité informatique préapprouvé par CNA a accepté de fournir aux assurés en cyberrisques de CNA une heure de consultation sans frais sur le processus de gestion des brèches de sécurité informatique.

Consultation pour les logiciels de rançon

L'entreprise MoxFive est un chef de file dans la gestion des cyberincidents et dans les conseils techniques, qui offre aux assurés en cyberrisques de CNA une heure de consultation sans frais sur le cycle de vie d'un incident par logiciel de rançon, de la prévention à la correction, en passant par la réaction. MoxFive met l'accent sur l'assistance préventive et aborde les meilleures pratiques à adopter pour prévenir les attaques de logiciels de rançon et y réagir, ainsi que pour mettre en place des sauvegardes solides et des solutions de reprise après sinistre.

Services de tarification préférentielle

Atténuation des logiciels de rançon

MoxFive propose une gamme complète de services conçus pour prévenir les attaques par logiciels de rançon, les atténuer et réagir en cas d'incident, et collabore avec les entreprises pour les conseiller sur les meilleures pratiques de l'industrie à adopter ainsi que pour mettre en place des sauvegardes solides, des stratégies et des solutions de reprise après sinistre qui répondent aux besoins des entreprises et aux exigences de sécurité actuelles.

Planification des interventions en cas d'incident

La planification des interventions en cas d'incident est primordiale pour la plateforme de cybersécurité d'une entreprise. La première question qu'une autorité de réglementation pose souvent après le signalement d'un incident est en effet de savoir si l'entreprise disposait ou non d'un plan d'intervention en cas d'incident. CNA a établi des partenariats avec de nombreux fournisseurs afin d'offrir un plan d'intervention en cas d'incident à tarif préférentiel.

Breach Plan Connect de NetDiligence ®

Breach Plan Connect®, développé par NetDiligence®, aide les assurés à élaborer un plan d'intervention en cas d'incident afin de réagir efficacement en cas de brèche de sécurité informatique. Le logiciel comprend un plan complet et pratique préinstallé, un rapport de suivi des incidents, une liste des interventions ainsi qu'une enquête gratuite de l'appréciation des cyberrisques. L'outil « Élaborez votre plan » (*Build Your Plan*) permet également d'adapter facilement le plan par défaut aux entreprises des assurés.

Caractéristiques principales

- Plateforme mobile conviviale : un accès au plan d'intervention en cas de brèche de sécurité informatique à tout moment, de n'importe où et sur n'importe quel appareil;
- Service hébergé : un accès à un plan d'intervention en cas de brèche de sécurité informatique même lorsque les systèmes d'une entreprise sont compromis ou dans l'impossibilité de fonctionner;
- Rappels programmés : la réception de courriels de rappel pour examiner et mettre à l'essai un plan d'intervention en cas de brèche de sécurité informatique
- Enquête gratuite de l'appréciation des risques : une évaluation et une comparaison des pratiques en matière de droit au domaine privé et de sécurité.

Avocats spécialisés en brèches de sécurité informatique : chaque membre du groupe d'avocats spécialisés en brèches de sécurité informatique préapprouvé par CNA est en mesure d'aider un assuré dans le cadre d'exercices de table. Plusieurs d'entre eux proposent des options d'exercices précis à taux fixe préférentiel aux assurés en cyberrisques de CNA.

Cabinets d'expertise judiciaire : en plus des options susmentionnées, plusieurs cabinets d'expertise judiciaire préapprouvés par CNA offrent des services liés aux plans d'intervention en cas de brèche de sécurité informatique à taux fixe préférentiel pour les assurés en cyberrisques de CNA.

Élaboration et révision des politiques et des procédures

L'élaboration de politiques et de procédures en matière de cybersécurité et de droit au domaine privé est essentielle à la plateforme de cybersécurité d'une entreprise. La deuxième question qu'une autorité de réglementation pose souvent après s'être renseignée sur le plan d'intervention en cas d'incident d'une entreprise est en effet de savoir si celle-ci a mis en place des politiques et des procédures appropriées en matière de sécurité et de droit au domaine privé. Les autorités de réglementation veulent également examiner lesdites politiques et procédures.

Avocats spécialisés en brèches de sécurité informatique : chaque membre du groupe d'avocats spécialisés en brèches de sécurité informatique préapprouvé par CNA est en mesure d'aider les assurés à élaborer, à réviser, à mettre à jour ou à rectifier les politiques et les procédures en matière de cybersécurité. Plusieurs d'entre eux proposent des services spécifiques liés aux politiques et aux procédures à taux fixe préférentiel aux assurés en cyberrisques de CNA.

Cabinets d'expertise judiciaire : en plus des options susmentionnées, plusieurs cabinets d'expertise judiciaire préapprouvés par CNA peuvent aussi préparer et examiner des politiques et des procédures en matière de sécurité à taux fixe préférentiel pour les assurés en cyberrisques de CNA.

Exercices de table

Lorsque les plans d'intervention en cas d'incident, les politiques et les procédures sont élaborés, les mettre correctement à l'essai est impératif. Les fournisseurs de Cyberprep de CNA sont disponibles pour effectuer diverses simulations de brèches de sécurité informatique et d'attaques afin de mettre à l'essai l'efficacité des interventions en cas d'incident ainsi que des plans de reprise après sinistre et de continuité des activités, et également de vérifier si les politiques et les procédures répondent correctement à des situations réelles.

Il est conseillé aux assurés de consulter leur courtier et leur souscripteur en cyberrisques de CNA pour en savoir plus sur chacun des services présentés dans la présente brochure.

Services de tarification préférentielle (suite)

Différents exercices de table existent. Certains exercices requièrent la participation d'un cabinet d'avocats ou d'un cabinet d'expertise judiciaire tandis que d'autres exigent la participation des deux. Le prix ainsi que le champ d'application des exercices de table varient selon l'option choisie.

Avocats spécialisés en brèches de sécurité informatique : chaque membre du groupe d'avocats spécialisés en brèches de sécurité informatique préapprouvé par CNA est en mesure d'aider un assuré dans le cadre d'exercices de table. Plusieurs d'entre eux proposent des options d'exercices précis à taux fixe préférentiel aux assurés en cyberrisques de CNA.

Cabinets d'expertise judiciaire : en plus des options susmentionnées, tous les cabinets d'expertise judiciaire préapprouvés par CNA peuvent aussi proposer des options d'exercice de table à taux fixe préférentiel pour les assurés en cyberrisques de CNA.

Tactiques, techniques et procédures de l'équipe rouge de CyberArk

Un engagement auprès de l'équipe rouge de CyberArk forme l'équipe des opérations de sécurité d'une entreprise aux attaques courantes que mènent les assaillants pour compromettre les contrôles de sécurité et mettre les entreprises en danger. Les équipes de sécurité accumulent l'expérience pratique dont elles ont besoin pour comprendre les techniques d'attaques populaires et les stratégies de défense.

Formation de sensibilisation à la sécurité

Les erreurs humaines restent l'une des principales causes de cyberincidents. Par conséquent, l'éducation et la formation des membres du personnel sont essentielles pour une plateforme de cybersécurité solide. CNA s'est associée au service de sécurité informatique Cofense pour offrir aux assurés en cyberrisques de CNA une formation de sensibilisation à la sécurité et aux campagnes d'hameçonnage.

Protection antivirus de nouvelle génération

L'antivirus Falcon Prevent de l'entreprise de cybersécurité Crowdstrike est un ensemble unique de méthodes efficaces destinées à prévenir les tactiques, les techniques et les procédures qu'utilisent les assaillants pour pénétrer les entreprises et dont l'évolution est rapide, notamment les logiciels malveillants de base, ceux de type « zero day » et même les attaques avancées sans utilisation d'un logiciel malveillant, et à s'en protéger.

Gestion des mots de passe

Une bonne gestion des mots de passe peut prévenir de nombreuses brèches de sécurité informatique, la mettre en place est donc essentiel. CNA s'est associée au gestionnaire de mots de passe Dashlane, un chef de file du secteur, pour offrir aux assurés de CNA l'un des meilleurs produits de gestion de mots de passe à tarif préférentiel.

Authentification multifacteur

L'authentification multifacteur (AMF) est un processus d'identification redondant, qui exige des utilisateurs qu'ils suivent plusieurs étapes pour accéder à un réseau ou à un système. Ce processus peut en effet comprendre une combinaison de mots de passe, de messages texte, de données biométriques ou d'autres méthodes d'identification. L'avantage de l'AMF est que plus les cybercriminels doivent franchir d'étapes liées à la sécurité pour accéder à un système, moins ils risquent d'essayer. CNA s'est également associée à la plateforme de gestion des identités Okta et à la plateforme de sécurité WatchGuard pour proposer différentes solutions d'AMF.

Produits de gestion des accès privilégiés de CyberArk

En plus de l'évaluation de la sécurité des accès à privilèges décrite dans la partie Identifier du présent document, les assurés en cyberrisques de CNA ont accès aux produits de gestion des accès à privilèges de CyberArk, notamment les produits suivants :

Découverte et audit (outil DNA) : un examen des besoins et des pilotes d'entreprise pour identifier les objectifs, les critères de réussite, les priorités et les cas d'utilisation d'une solution de sécurité des accès à privilèges. Grâce à CyberArk, la clientèle mène un examen approfondi des contrôles essentiels et des délais à l'aide des cadres d'application et des outils de CyberArk tels que le programme d'hygiène informatique de la sécurité des accès à privilèges de CyberArk et l'outil Découverte et audit (DNA).

Outil d'élaboration de programme de CyberArk : les conseillers de CyberArk, chefs de file du secteur, aident à planifier et à élaborer des programmes de sécurité des accès à privilèges. Grâce à leur offre, la formulation d'un programme est plus rapide, économique et permet de gagner du temps, faisant passer le délai d'élaboration de plusieurs mois à quelques semaines.

Il est conseillé aux assurés de consulter leur courtier et leur souscripteur en cyberrisques de CNA pour en savoir plus sur chacun des services présentés dans la présente brochure.

Services de tarification préférentielle (suite)

Sécurisation des terminaux et planification de la stratégie de droit d'accès minimal

L'escalade des privilèges est au cœur de la plupart des cyberattaques et de la vulnérabilité des systèmes. Pourtant, de telles brèches de sécurité informatique peuvent facilement être évitées, en appliquant le principe de « droit d'accès minimal », qui est l'un des fondements de l'architecture d'entreprise zéro confiance. Celui-ci s'applique aux environnements des serveurs, aux postes de travail des utilisateurs et aux pupitres de commande pour les machines et objets connectés des usines de l'industrie 4.0, afin de mettre en place des mesures de sécurité dès la conception.

L'éditeur de logiciels de sécurité informatique WALLIX propose BestSafe, une solution applicative de sécurité innovante qui permet aux entreprises de supprimer complètement les comptes administrateurs, de réduire considérablement les failles de sécurité sans nuire à la productivité et de se conformer plus facilement avec les directives réglementaires. De plus, si BestSafe est associé à la ligne de produits Bastion (Wallix PAM), il contribue à accorder les privilèges aux applications et non aux utilisateurs lorsque la situation l'exige, préservant ainsi l'architecture zéro confiance.

Il est conseillé aux assurés de consulter leur courtier et leur souscripteur en cyberrisques de CNA pour en savoir plus sur chacun des services présentés dans la présente brochure.

Réagir

Les titulaires de polices d'assurance continuent de profiter de CyberPrep de CNA au fil du temps. En cas de brèche de sécurité informatique, un groupe de fournisseurs de CNA à l'efficacité prouvée en matière de **réponse à un incident** prodigue des conseils et propose des stratégies pour accélérer la reprise et atténuer les pertes. Les services offerts englobent des conseils en cas de brèche de sécurité informatique, des spécialistes en expertise judiciaire, des services de notifications et de surveillance du crédit, ainsi que de relations publiques.

Avocats spécialisés en brèches de sécurité informatique : chaque membre du groupe d'avocats spécialisés en brèches de sécurité informatique préapprouvé par CNA peut déterminer si des renseignements confidentiels ont été consultés et si diverses lois provinciales ou territoriales ont été invoquées exigeant une notification à la clientèle à la suite d'une violation de données. Les avocats spécialisés en brèches de sécurité informatique peuvent également aider la clientèle à interpréter les diverses réglementations ainsi que les responsabilités des assurés en vertu de la loi (s'il y a lieu), et à rédiger une déclaration.

Cabinets d'expertise judiciaire : les cabinets d'expertise judiciaire préapprouvés par CNA apportent leur aide dans le cadre de l'enquête à la suite d'une brèche de sécurité informatique ainsi que des mesures correctives, notamment en déterminant les faits qui entourent la violation de données et en contribuant à la compréhension de l'étendue de l'incident.

Services de notification et de surveillance du crédit : les fournisseurs approuvés par CNA offrent à la clientèle des assurés des services de surveillance du crédit après une brèche de sécurité informatique.

Relations publiques : les fournisseurs de relations publiques approuvés par CNA aident les assurés dans leurs efforts de communication publique et de publicité potentielle après une brèche de sécurité informatique.

Les assurés doivent se référer à l'aperçu Assistance en cas d'intrusion informatique de CNA ou à l'onglet post brèche de sécurité informatique (« post-breach ») sur le portail Web eRiskHub® pour en savoir plus sur ces entreprises et cabinets ainsi que leurs services.

Il est conseillé aux assurés de consulter leur courtier et leur souscripteur en cyberrisques de CNA pour en savoir plus sur chacun des services présentés dans la présente brochure.

Assistance en cas d'incident informatique lié à la protection des renseignements personnels

Vous assurer en ligne, hors ligne et partout dans le monde

CNA a identifié un réseau de consultants et de consultantes, de cabinets d'expertise judiciaire et de fournisseurs de centres de notification et d'appels à l'efficacité prouvée qui peuvent vous venir en aide pour réagir rapidement et de manière appropriée en cas d'incident lié à la protection des renseignements personnels. CNA sait que chaque situation est unique et son équipe spécialiste des sinistres travaille à vos côtés pour choisir les fournisseurs qui conviennent le mieux à vos besoins particuliers.

Fournisseurs privilégiés de CNA en matière d'incidents liés à la protection des renseignements personnels :

Avocats spécialisés en brèches de sécurité informatique

Bell Temple LLP
Katherine E. Kolnhofer
kkolnhofer@belltemple.com
416-581-8213
24/7 Courriel : cyberbreach@belltemple.com
24/7 Téléphone : 416-581-1303

Norton Rose Fulbright Canada LLP
Imran Ahmad
imran.ahmad@nortonrosefulbright.com
416-863-4329
24/7 Courriel : nrfc.breach@nortonrosefulbright.com
24/7 Téléphone : 1 866 BREACHX (1 866-273-2249)

Clyde & Co
Nathalie David
nathalie.david@clydeco.ca
514-764-3611
24/7 Courriel : cyberresponseline.canada@clydeco.com
24/7 Téléphone : 514-907-7444

Bennett Jones LLP
Gary Solway
solwayg@bennettjones.com
416-777-6555
24/7 Courriel : bjresponse@bennettjones.com
24/7 Téléphone : 416-777-5500

Dolden Wallace Folick LLP
Mercy Iannicello
miannicello@dolden.com
604-891-0373
24/7 Courriel : cnacyber@dolden.com
24/7 Téléphone : 1 888-701-7832

Cabinets d'expertise judiciaire

Arete Incident Response
Brookes Taney
1 866-210-0955
arete911@areteir.com

Charles River Associates
Aniket Bhardwaj
416-323-5574
abhardwaj@crai.com

Kroll
Wayne Hayes-Heath
wayne.hayesheath@kroll.com
cyberresponse@kroll.com

CrowdStrike
Adam Cottini
adam.cottini@crowdstrike.com
1 855-276-9347
services@crowdstrike.com

Kivu Consulting, Inc.
Cristin Sinnott
csinnott@kivuconsulting.com
1 855-548-8767
incidentresponse@kivuconsulting.com

Services de notification et de surveillance du crédit

AllClearID
1 877-736-4486

Equifax
Allen Burzen
allen.burzen@equifax.com
512-650-6285

TransUnion
dca@transunion.ca

Epiq
Cameron Azari
caza@epiqglobal.com

Experian
Ozzie Fonseca
ozzie.fonseca@experian.com
949-567-3851

Relations publiques

FleishmanHillard HighRoad
fhhighroad.com
416-214-0701

À propos de CNA

CNA est l'une des plus importantes compagnies d'assurance de dommages des entreprises aux États-Unis. Forte de plus de 125 ans d'expérience, CNA offre une vaste gamme de produits et de services d'assurance standards et spécialisés aux entreprises et aux professionnels aux États-Unis, au Canada et en Europe.

Pour en savoir plus, veuillez consulter le site Internet de CNA à l'adresse cnacanada.ca.