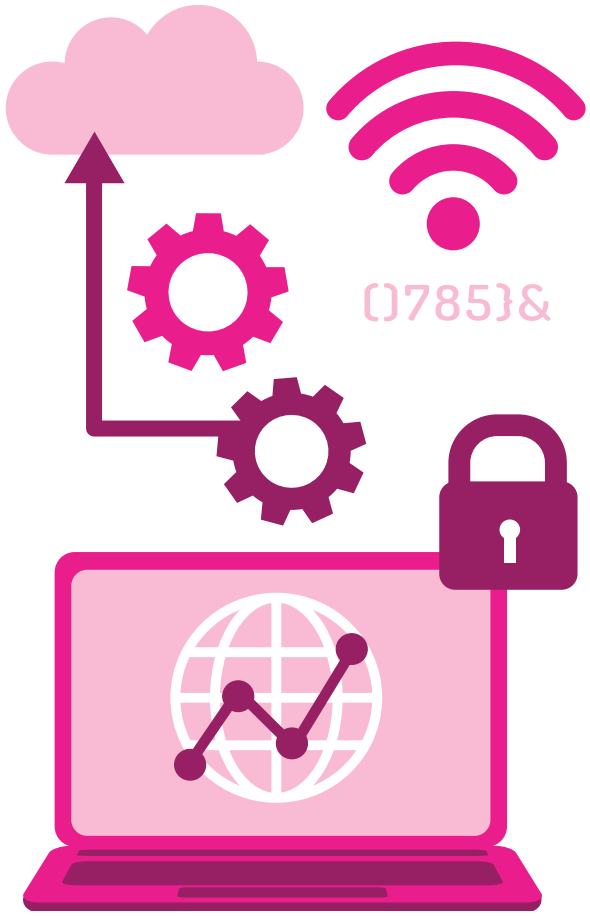
CHUBB®

Guide de gestion des risques cyber pour les courtiers

Ce guide comprend des informations sur :

1. Pourquoi le risque cyber est important ?
2. Expositions par secteur
3. TPE
4. PME et ETI
5. Grandes entreprises
6. Principaux arguments de vente
7. Services de prévention des risques
8. Services de réponse à incident
9. Contrat Garantie Cyber ERM
10. Appétits

Pourquoi le risque cyber est important ?



A l'ère de l'information et du numérique, nous collectons toujours plus de données, dans le monde entier 24h/24 et 7j/7 et collaborons de manière plus efficace ; le digital simplifie les processus des entreprises.

La dépendance accrue vis-à-vis des systèmes informatiques et l'accès aux informations peut aggraver de manière significative la vulnérabilité d'une entreprise face aux menaces relatives à la cybersécurité. Les pannes, les erreurs et les attaques affectant les nouveaux modes de gestion / fabrication peuvent entraîner des frais significatifs avec un impact très important sur la rentabilité de l'entreprise. En ce qui concerne les atteintes à la sécurité des données ou la perte de confidentialité, il ne s'agit pas de savoir si cela va se produire mais plutôt de quand cela va se produire. Si cela survient, vous aurez besoin d'une protection adaptée de la part d'un assureur spécialisé dans la gestion des risques cyber, qui propose une gamme complète de solutions d'assurance intégrées pour aider à combler les insuffisances de garanties, et qui peut personnaliser son offre selon votre activité. Depuis 1998, Chubb propose des solutions d'assurance Cyber à ses assurés.

Les limites des assurances traditionnelles

Les entreprises pensent souvent que leurs polices d'assurance existantes suffisent à couvrir les expositions en termes de sécurité des données et de confidentialité. Malheureusement, il en est autrement et les polices d'assurances traditionnelles ne prennent pas en compte l'intégralité de ses expositions qui menacent les entreprises aujourd'hui. Les polices d'assurance traditionnelles sont les suivantes :

Responsabilité civile générale

Le recours aux polices de Responsabilité civile générale survient généralement suite à des réclamations de tiers concernant des dommages corporels (DC) et des dommages matériels (DM). En général, un incident cyber ne va pas engendrer de dommage coporel ou matériel. D'ailleurs, les polices de responsabilité civile générale ne prévoient pas la couverture des dommages (corporels ou matériels) subis par l'entreprise/les salariés de l'entreprise.

Dommage aux biens

Le recours aux polices d'assurance dommages aux biens survient en général suite à un dommage matériel affectant les biens de l'entreprise et pouvant être causés par un incendie, dégât des eaux ou autre type d'événement. Suite à un événement qui affecte les biens de l'entreprise, il peut aussi y avoir un impact en termes de résultats financiers. La perte d'exploitation et les frais supplémentaires couvrent les pertes subies par l'entreprise. Un incident cyber, ne causera pas de dommages matériels. Néanmoins,il peut conduire dans certains cas à la fermeture de l'entreprise.

Fraude

Le recours aux polices d'assurance Fraude survient suite à des pertes financières subies dues à un acte frauduleux (vol d'argent, de titres, de bien corporels) commis par un préposé ou un tiers . Les extensions concernant la cybercriminalité excluent en général la couverture de Responsabilité civile et peuvent être insuffisantes pour couvrir la perte d'informations confidentielles.

Expositions par secteur

Établissements financiers

Les institutions financières sont fortement exposées aux risques cyber en raison d'un certain nombre de facteurs. La cybercriminalité, l'activisme des hackers et des spécialistes du cybercrime aux techniques toujours plus sophistiquées menant des activités d'espionnage pour le compte d'un commanditaire ne représentent qu'une partie des risques à prendre en compte. La vulnérabilité aux incidents cyber peut s'avérer très élevée car de nombreuses institutions financières dépendent de réseaux hautement interconnectés et d'infrastructures critiques. En raison de leur forte dépendance vis-à-vis de la technologie, la plupart des institutions financières continueront de voir grandir leur exposition aux risques

Sinistres courants : Ingénierie Sociale – Hameçonnage et Erreur humaine

Secteur de la santé

La très forte montée en puissance de la numérisation des dossiers médicaux a eu pour conséquence une dépendance accrue des entreprises du secteur de la santé vis-à-vis de systèmes informatiques pour la collecte et le traitement de données personnelles de santé et médicales extrêmement sensibles. Il existe une exposition forte aux erreurs administratives car on attend des employés qu'ils saisissent des informations précises dans les systèmes. Les systèmes informatiques traditionnels sont souvent interconnectés avec le reste du réseau de l'entreprise, ce qui augmente le potentiel pour qu'un incident ait un impact sévère sur les opérations.

Sinistres courants : Erreur humaine et utilisation frauduleuse des systèmes d'information

Vente au détail

Qu'il s'agisse d'une entreprise digitale ou d'une société traditionnelle, l'historique sinistre de Chubb montre que le secteur de la vente au détail est fortement exposé aux pertes liées aux risques cyber. Les entreprises de vente au détail possèdent souvent de nombreux sites qui peuvent ou non : opérer sur des systèmes informatiques centralisés, avoir une dépendance vis-à-vis d'un réseau de fournisseurs de services informatiques, avoir une potentielle dépendance aux sites Internet en raison de l'augmentation des ventes en ligne des données personnelles et sensibles due à la fréquence élevée des transactions financières et des programmes de fidélité.

Sinistres courants : Piratage et Ingénierie Sociale – Hameçonnage

Hôtellerie

L'industrie hôtelière regroupe un large éventail d'opérations telles que les hôtels, les bars ou encore les restaurants. Dans cette activité, les expositions liées aux risques cyber comprennent : des volumes importants d'informations de consommateurs et d'employés, une dépendance souvent forte des sites Internet pour les réservations client, des informations sur les programmes de fidélité qui peuvent mener à des problèmes de confidentialité car ils peuvent être la cible d'attaques par ingénierie sociale et d'hameçonnage.

Sinistres courants : Ingénierie Sociale – Hameçonnage et piratage

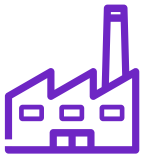
Services professionnels

Compte tenu de la quantité de données confidentielles collectées par les sociétés de services , le secteur des services aux entreprise ou aux particuliers constitue une cible privilégiée pour les cyberattaques. Par exemple, les informations et les fonds qu'un cabinet d'avocats ou un cabinet comptable détiennent peuvent se révéler lucratifs pour un cybercriminel. Par ailleurs, les conséquences en matière de réputation pour une société victime d'une atteinte à ses données peuvent être hautement préjudiciables. Le stockage massif de données sensibles de clients a entraîné l'augmentation des incidents cyber affectant les entreprises de services aux particuliers ou aux entreprises ces dernières années

Sinistres courants : Erreur humaine et piratage

*Les causes courantes de déclarations de sinistres sont extraites du Cyber Risk Index℠ de Chubb

Expositions par secteur



Secteur manufacturier

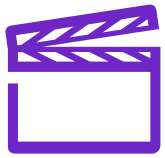
Le secteur manufacturier est l'un des principaux secteurs d'activité ciblé par les cybercriminels. Le recours de plus en plus important aux technologies de l'information change la manière dont les industriels exercent leurs activités. Pour améliorer la productivité et la rentabilité, de nombreux producteurs industriels exploitent l'Internet des objets (IdO), la numérisation et les services Cloud, augmentant ainsi l'impact de certains incidents cyber. De récents incidents affectant les systèmes de contrôle industriel (Industrial Control Systems, ICS) et les systèmes de surveillance et d'acquisition de données (Supervisory Control and Data Acquisition, SCADA) ont mené à un arrêt total des opérations de certaines usines.

Sinistres courants :
Logiciel malveillant et
Ingénierie sociale – Hameçonnage

Enseignement

L'enseignement de façon générale est vulnérable en raison des données sensibles que les établissements détiennent relatives aux étudiants ainsi qu'au personnel. Les écoles et universités ont souvent des budgets et ressources limités dédiées à l'informatique. Les menaces sont à la fois externes et internes, qu'il s'agisse d'un étudiant introduisant un logiciel malveillant sur le réseau intentionnellement ou par inadvertance, ou d'un membre du personnel ne respectant pas les règles de sécurité en vigueur, entraînant une violation de données.

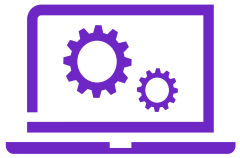
Sinistres courants :
Ingénierie sociale -
Hameçonnage et Piratage



Médias/Divertissement

Les sociétés de médias, loisirs ou divertissement font souvent l'objet de menaces de cyber extorsion ciblant des documents ou contenus sensibles. Des attaques par déni de service distribué (Distributed Denial of Service, DDoS) ou des pannes de systèmes informatiques peuvent sérieusement affecter des activités de diffusion et/ou livraisons de contenu. La détention d'informations personnelles sensibles concernant les abonnés aggrave l'exposition.

Sinistres courants :
Erreur humaine et
Ingénierie sociale – Hameçonnage



Technologie

Les entreprises de technologie sont considérées comme fiables par leurs clients qui voient en elles des leaders dans les secteurs de la cybersécurité et la protection des données, ce qui augmente le risque d'atteinte à la réputation de l'entreprise en cas d' incident cyber. Les incidents cyber arrivant dans des société technologiques peuvent également affecter la couverture des Erreurs et omissions liées aux technologies. Veuillez contacter votre souscripteur Chubb pour obtenir plus d'informations sur notre offre combinée Responsabilité Professionnelle et cyber, destinée aux entreprises technologiques.

Sinistres courants :
Piratage et Erreur humaine

*Les causes courantes de sinistres cyber sont extraites t du Cyber Risk Index℠ de Chubb

Voir ce que Chubb peut proposer aux entreprises de toutes tailles pour faire face à ces expositions :

TPE

PME et ETI

Grandes entreprises

TPE - Vue d'ensemble

Malgré une plus large médiatisation des incidents cyber affectant les grandes entreprises, les PME et ETI sont aussi souvent concernées par des menaces et impactées suite à l'exploitation de failles de sécurité. Les TPE sont souvent perçues comme des cibles plus faciles par les cybercriminels en raison de leurs ressources et investissements informatiques souvent limités.

En outre, elles consacrent en général moins de temps et de ressources dans la formation du personnel concernant la sécurité des données, la mise en place d'une politique de mots de passe et l'authentification à deux facteurs. Les PME et ETI représentent souvent une opportunité lucrative pour les cybercriminels par rapport à des entreprises plus grandes et mieux protégées. Elles doivent également prendre conscience que même sans être la cible initiale, elles peuvent être affectées par un incident survenu chez un prestataire informatique externe ou un partenaire commercial.

Sinistres affectant les TPE - Chubb Cyber Index℠

Les exemples concrets et données plus générales consistuent la meilleure manière d'illustrer les risques cyber auxquels sont confrontées les petites entreprises. Chubb traite des sinistres cyber depuis plus de vingt ans. Dans le cadre du processus de déclaration de sinistre, nous suivons des indicateurs clés tels que les actions causant une perte de données, le fait que l'incident cyber soit causé par un acteur interne ou externe, le nombre de données affectées et la taille et le secteur d'activité de l'assuré impacté. Nous publions le Chubb Cyber Index℠ pour communiquer avec nos clients et courtiers et les informer des tendances en matière de sinistres cyber.

Le Chubb Cyber Index℠ fournit aux utilisateurs un moyen d'identifier les principaux risques cyber auxquels leur entreprise fait face en se basant sur des exemples réels de cyberattaques et de fuites de données. Les utilisateurs peuvent définir les paramètres et observer les tendances historiques en fonction du type de menace, de la taille de l'entreprise et de son secteur d'activité.

Pour en savoir plus, rendez-vous sur le Chubb Cyber Index℠ ici :
https://chubbcyberindex.com

TPE - Scénarios de sinistres

Rançongiciel

Notre assuré, une entreprise de construction, a été victime d'une attaque ciblée par rançongiciel. L'accès aux systèmes de l'assuré a été piraté après qu'un employé ait cliqué sur un lien frauduleux dans un e-mail. Les systèmes et serveurs de l'assuré ont été chiffrés puis une demande de 800 000 CHF en bitcoins a été exigée. L'assuré a fait appel à l'équipe de réponse à incident mise à disposition par Chubb, laquelle a diligenté l'envoi de spécialistes en investigation informatique, dans le but de comprendre le mécanisme et la portée de l'attaque. L'assuré ayant choisi de ne pas payer la rançon, l'ensemble de l'activité de l'assuré a été perturbée pendant plus de six mois.

Garantie applicable :

Remise en état des données et des systèmes, pertes d'exploitation, frais de réponse à incident et frais liés à la cyber extorsion.

Prévention

Revue régulière des mesures de sécurité informatique, formation des employés, sauvegarde régulière des données, et plans de réponse à incident et/ou de continuité des activités en place.

Employé malveillant

Notre assuré a été victime d'un employé malveillant qui a volé plus de 700 données personnelles de clients, comprenant notamment leurs noms, adresses et contacts. Elles ont été fournies au nouvel employeur pour qu'il les utilise à son avantage. Cet incident s'étant produit après la mise en place du RGPD, il a fallu le notifier à l'autorité de contrôle des données personnelles.

Garantie applicable :

Responsabilité civile vie privée et frais de réponse à incident.

Prévention

Il est extrêmement difficile d'empêcher des employés mal intentionnés de causer des dommages. Ils ont le plus souvent accès aux systèmes nécessaires leur permettant de subtiliser des données sensibles concernant l'entreprise elle-même ou des personnes physiques. Au vu de la jurisprudence actuelle, il est probable que l'entreprise soit tenue responsable vis-à-vis de ses clients. La solution d'assurance cyber Chubb fournit les outils nécessaires pour faire face aux problèmes quand ils surviennent.

Erreur d'un employé

Notre assuré, une association régionale de logement au Royaume-Uni, a subi par inadvertance une violation de données à la suite de l'erreur d'un employé. En publiant une nouvelle annonce pour un logement vacant, l'employé a par erreur inclus l'image du dossier médical d'un autre client dans la brochure en ligne.

Garantie applicable :

Responsabilité civile vie privée et frais de réponse à incident.

Prévention

Il est important d'avoir une politique de confidentialité à l'échelle de l'entreprise détaillant les process de sécurité relatifs au traitement des informations sensibles. Les employés devraient rendre compte de leur compréhension de la conformité à cette politique et la reconnaître officiellement au moins une fois par an.

TPE - Scénarios de sinistres

Accès non autorisé – Hameçonnage

Notre assuré, une entreprise de logistique, a été victime d'une attaque de type hameçonnage à travers un logiciel malveillant. Un employé au sein de l'équipe RH de l'assuré a vu apparaître une fenêtre contextuelle sur son écran d'ordinateur après avoir cliqué sur un lien frauduleux dans un e-mail. La fenêtre indiquait que l'ordinateur était infecté et qu'il était nécessaire d'appeler le numéro de téléphone indiqué. Les fraudeurs ont ensuite obtenu un accès à distance à l'ordinateur de l'employé grâce à l'ingénierie sociale.

Garantie applicable :

Responsabilité civile vie privée, responsabilité civile sécurité des réseaux et frais de réponse à incident.

Prévention

Même avec les meilleurs technologies et systèmes de sécurité, la plus grande vulnérabilité d'un assuré a trait à son personnel. Le personnel peut être amené par la tromperie à fournir des mots de passe ou des accès. Une formation régulière sur l'hameçonnage est conseillée, et il devient essentiel d'avoir une police d'assurance qui fournira l'expertise extérieure nécessaire en cas d'incident cyber.

Perte de données physiques

Notre assuré, un cabinet d'avocats, a contacté le service d'assistance Chubb de réponse à incident quand il s'est avéré qu'un employé de la société avait enfreint le protocole en sortant du bureau des dossiers de clients et en les conservant dans sa voiture. Le véhicule a par la suite été volé et les dossiers des clients perdus.

Garantie applicable :

Responsabilité civile vie privée et frais de réponse à incident.

Prévention

Ayez en place un processus clair concernant la conservation des données numériques et physiques. La sauvegarde régulière des données est importante pour assurer une reprise d'activité rapide après la survenance d'un incident. Créez une politique de confidentialité à l'échelle de l'entreprise que les employés doivent reconnaître et accepter.

TPE - Une solution de cybersécurité sur mesure

1 Services de prévention des risques pour les TPE

Pour aider nos TPE assurées à réduire les effets d'un sinistre cyber, Chubb propose plusieurs services gratuits ou à prix très réduit.

Les solutions de gestion de mots de passe sont gratuites pour les assurés ayant au maximum 500 employés.

- Une gestion efficace des mots de passe peut aider à réduire le risque d'une utilisation non autorisée d'identifiants volés.

Des formations de sensibilisation au risque d'hameçonnage sont disponibles pour les assurés.

- L'hameçonnage est une des causes de dommages cyber qui croit le plus rapidement et une formation simple des employés peut s'avérer un outil efficace pour éviter une attaque par hameçonnage.

Cliquer ici pour obtenir plus d'informations sur notre gamme complète de services cyber, notamment les services de cybersécurité et plus encore.

2 Services de réponse à incident pour les petites entreprises

Chez Chubb, nous savons qu'il est impossible d'éviter tous les incidents. Quand un incident survient, nos polices cyber permettent aux TPE de bénéficier de l'accompagnement d'une équipe d'intervention en cas d'incident, et ce sans franchise.

Ces spécialistes sont disponibles 24h/247j/7et 365 j/an , et vous accompagnent dans le processus de résolution de l'incident.

- Les experts regroupent la gestion de réponse à incident, les frais d'investigations informatiques (forensics), les conseils juridiques et réglementaires, la communication de crise et autres.
- L'accès au réseau de fournisseurs est inclus dans la police.
- Disponibles 24h/24, 7j/7 et 365j/an via l'appli Cyber Alert®, téléphone ou le site Internet.
- Ils peuvent fournir une assistance à la suite de tout incident cyber réel ou seulement suspecté : ils sont là pour aider dans toute situation urgente.

Cliquez ici pour obtenir plus d'informations sur le fonctionnement de la solution de réponse à incident de Chubb.

3 Souscription en ligne pour TPE

La plateforme en ligne Chubb Easy Solutions a été spécialement conçue pour les courtiers. Elle permet d'établir des devis et mettre en place les garanties pour les TPE. En alliant une solution intuitive à une expérience centrée sur le client, les courtiers peuvent mettre en place les garanties cyber et transmettre les documents contractuels au client en quelques minutes.

La plateforme permet de bénéficier des mêmes avantages que la souscription des risques sur-mesure :

- Questionnaire simplifié
- Peu de secteurs d'activité exclus pour les TPE
- Même texte de garantie qu'en sur-mesure
- Accès aux services de prévention des risques de Chubb
- Modification des dates, limites, taux de commission et informations sur la police sans avoir à contacter le souscripteur
- Devis et mise en place des garanties en quelques minutes

Contactez votre souscripteur Chubb local pour découvrir les différentes solutions de souscription en ligne ou d'autres solutions simplifiées pour les TPE.

PME et ETI - Vue d'ensemble

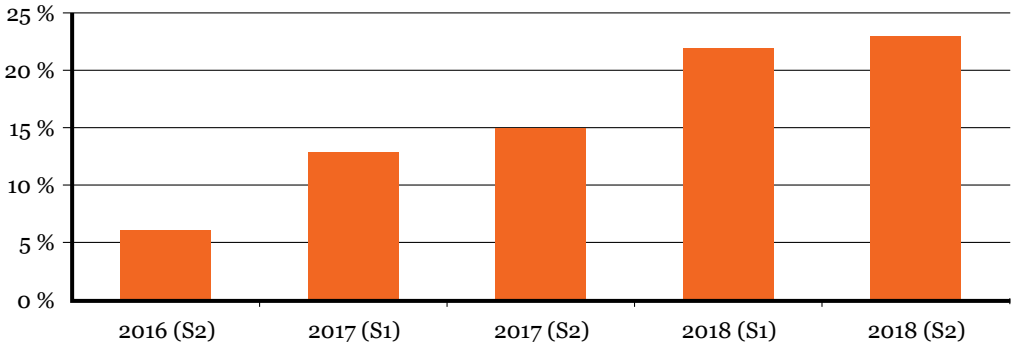
Les PME et ETI sont confrontées aux mêmes problématiques de cybersécurité que les grandes entreprises mais ont moins de budget IT et moins de personnel spécialisé pour gérer ce risque. Elles ont souvent la même vision que de nombreuses TPE, pensant que seules les grandes entreprises font face à un risque important. Les activités malveillantes devenant de plus en plus sophistiquées, les PME et ETI ont de plus en plus de difficultés à se défendre.

Chubb Cyber Index℠

L'index fournit aux utilisateurs un moyen d'identifier les principaux risques cyber auxquels leur entreprise est confrontée en se basant sur des cas concrets de cyberattaques et de violation de données. Les utilisateurs peuvent définir les paramètres et observer les tendances historiques en fonction du type de menace, de la taille de l'entreprise et de son secteur d'activité .

Pour en savoir plus, cliquez sur le Chubb Cyber Index℠ ici :
https://chubbcyberindex.com

Sinistres Chubb comparés au S1 2016 (taux de croissance)
PME et ETI - Tous secteurs d'activité



PME et ETI - Scénarios de sinistres

Rançongiciel

Une résidence médicalisée a connu une attaque par « force brute » avec rançongiciel et a vu plusieurs de ses fichiers chiffrés. Une rançon d'environ 26 000 CHF a été initialement demandée. Après le paiement d'une partie de la rançon permettant d'obtenir un échantillon de l'outil de déchiffrement des données, la société a décidé de s'appuyer plutôt sur ses sauvegardes pour restaurer ses systèmes.

Garantie applicable :

Remise en état des données et du système, perte d'exploitation, frais de réponse à incident et frais liés à la cyber extorsion.

Prévention

Le fait d'investir dans les technologies de sécurité, bien qu'étant essentiel pour aider à la prévention contre les accès non autorisés, n'est pas un rempart infaillible. Les attaquants font sans cesse évoluer leurs méthodes, et toute entreprise doit vérifier régulièrement sa sécurité et ses procédures pour rester à jour face aux menaces.

Erreur d'un employé

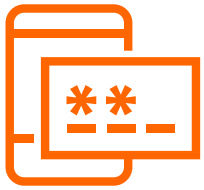
Un employé d'un revendeur de matériel informatique a ignoré les politiques et procédures internes et a ouvert une pièce jointe d'apparence inoffensive dans un e-mail. Le lendemain, les commandes de stock et les caisses enregistreuses du magasin ont commencé à dysfonctionner et l'activité commerciale s'est dégradée en raison d'une panne du réseau.

Garantie applicable :

Remise en état des données et du système, responsabilité civile en cas d'atteinte à la sécurisation des réseaux, perte d'exploitation et frais de réponse à incident.

Prévention

Former régulièrement pour s'assurer que le personnel est informé de ce qu'il faut vérifier dans les pièces jointes d'e-mails suspicieux, et la procédure à suivre en cas de doute. En outre, un accès immédiat à un coordinateur de réponse à incident et un panel de spécialistes permettra une intervention rapide pour gérer cette situation.



Violation de données

Le réseau informatique d'un hôtelier a été piraté, ce qui a potentiellement compromis la sécurité de tous les dossiers appartenant à la fois aux employés et aux clients, y compris les informations de cartes bancaires des clients.

Garantie applicable :

frais de réponse à incident, remise en état des données et du système, et responsabilité civile en cas d'atteinte à la confidentialité des données et la sécurisation des réseaux.

Prévention

Le système de détection d'intrusion est un outil précieux pour lutter contre un pirate informatique. Cela permet de repérer rapidement toute activité suspicieuse. Le chiffrement des données est également primordial pour protéger les données et éviter qu'elles soient facilement supprimées et utilisées.

PME et ETI - Scénarios de sinistres

Minage de crypto-monnaies

Une entreprise manufacturière a connu une attaque par rançongiciel qui a eu pour conséquence un chiffrement de plusieurs de leurs fichiers. Après que l'assuré a contacté Chubb via la ligne de réponse à incident 24h/24, 7j/7, nous avons proposé une consultation avec un coordinateur de réponse à incident et des experts juridiques de notre panel d'experts en cybersécurité. Suite à ces discussions, l'assuré a choisi de ne pas payer la rançon. Cependant, quand l'entreprise d'investigation informatique (forensic) a commencé à travailler à la résolution de l'attaque du rançongiciel, elle a découvert que l'assuré était également victime de minage de crypto-monnaie. Les attaquants avaient installé un logiciel dans le système de l'assuré qui minait des Bitcoins.
Le minage de crypto-monnaies se produit lorsque le système informatique d'une tierce partie est utilisé pour le minage à leur insu.

Garantie applicable :

frais de réponse à incident, perte d'exploitation, remise en état des données et du système, et responsabilité civile en cas d'atteinte à la confidentialité et et la sécurisation des réseaux.

Prévention

Une vérification régulière de la sécurité informatique est importante pour qu'un industriel s'assure que la production ne soit affectée par une attaque. Il doit envisager un plan de reprise d'activité et un plan de continuité d'activité permettant, en cas d'attaque, de réduire les perturbations. L'accès non autorisé n'est pas une technique infaillible. Les attaquants font sans cesse évoluer leurs méthodes, et toute entreprise doit vérifier régulièrement sa sécurité et ses procédures pour rester à jour face aux menaces.

Vol de données qui aboutit à l'extorsion, à l'interruption des activités et à des frais supplémentaires

Une organisation inconnue a piraté le réseau d'un cabinet d'avocats et a pu avoir accès à des informations client sensibles, notamment la cible d'acquisition d'une entreprise publique, la future technologie brevetée d'une autre entreprise publique, une version provisoire de la brochure d'un client en capital-risque, et un nombre important de données concernant les class-action (données personnelles sur les demandeurs). Un expert informatique (forensic) embauché par le cabinet d'avocats a déterminé qu'un logiciel malveillant avait été introduit dans son système. Peu de temps après, le cabinet a reçu un appel de l'attaquant réclamant 10 millions USD pour éviter la divulgation sur Internet des informations volées. Le cabinet d'avocats a engagé des dépenses de 2 millions USD pour une investigation juridique, des négociations liées à l'extorsion, un paiement de rançon, des notifications, une surveillance de l'utilisation frauduleuse de moyens de paiement et d'usurpation d'identités , des services de restauration des données et des frais de conseil juridique indépendant.

Garantie applicable :

Cyber extorsion, responsabilité civile en cas d'atteinte à la confidentialité et la sécurisation des réseaux, perte d'exploitation, et frais de réponse à incident.

Prévention

Il est important de former le personnel pour empêcher toute ouverture d'e-mail frauduleux. En outre, une solution informatique doit être mise en place pour détecter les logiciels malveillants lorsqu'ils passent entre les mailles du filet.

PME et ETI - Une solution cyber sur mesure

1 Services de prévention des risques pour les PME et ETI

Pour accompagner nos assurés du marché des TPE à atténuer les principaux risques de sinistres cyber, Chubb propose plusieurs services gratuits et à prix très réduits.

Les solutions de gestion de mots de passe sont gratuites pour un maximum de 100 employés pour chaque assuré.

- Une gestion efficace des mots de passe peut aider à minimiser l'utilisation non autorisée d'identifiants volés.

Des simulations de formation sur l'hameçonnage sont disponibles pour les assurés.

- L'hameçonnage est une des causes d'incident cyber qui croît de plus en plus. Une sensibilisation des employés peut s'avérer efficace pour réduire les attaques d'hameçonnage au sein de PME et ETI.

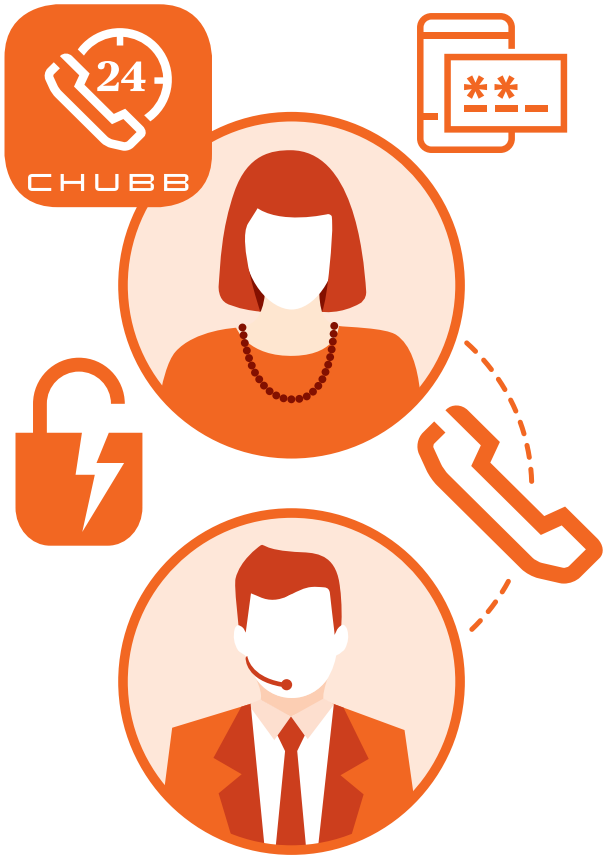
Cliquez ici pour obtenir plus d'informations sur notre suite complète de services cyber, notamment les services de cybersécurité.

2 Services de réponse à incident pour les PME et ETI

Répondre rapidement et de manière efficace à un incident cyber est capital pour en diminuer l'impact et les dommages. Dans les cas où un incident survient, nos polices cyber prévoient de mettre en relation nos assurés du secteur des PME et ETI à un panel d'experts en services de réponse à incident. Ces spécialistes sont disponibles 24 h/24, 7 j/7 et 365 j/an, et ils vous accompagnent dans la remise en état de vos systèmes après tout incident cyber.

- Le panel d' experts comprend la gestion de réponse à incident, l'expertise informatique judiciaire, les cabinets d'avocat, des experts en relations publiques ainsi que des négociateurs spécialisés en cyber extorsion.
- Flexibilité pour utiliser notre panel de fournisseurs ou tout fournisseur avec qui vous avez déjà établi un contrat dans le cadre d'un plan de réponse à un incident cyber.
- Disponible 24h/24, 7j/7 et 365j/an via l'appli Cyber Alert®, ligne téléphonique gratuite ou site Internet.
- « Réponse en urgence à incident » fournit une assistance à la suite de tout incident cyber réel ou seulement suspecté : l'équipe est là pour apporter un service d' urgence en cybersécurité sans application d'une quelconque franchise pendant 48 heures.

Cliquez ici pour obtenir plus d'informations sur le fonctionnement des services de réponse à incident de Chubb.



PME et ETI - Une solution cyber sur mesure

3 Services d'ingénierie des risques

La manière d'opérer d'un client et la technologie qu'il utilise peuvent différer en fonction des process et métiers. Nos ingénieurs en risques cyber aident les clients à identifier et à comprendre leurs vulnérabilités technologiques et les aident dans la prévention d'un futur incident cyber avant même la mise en place de la police d'assurance.

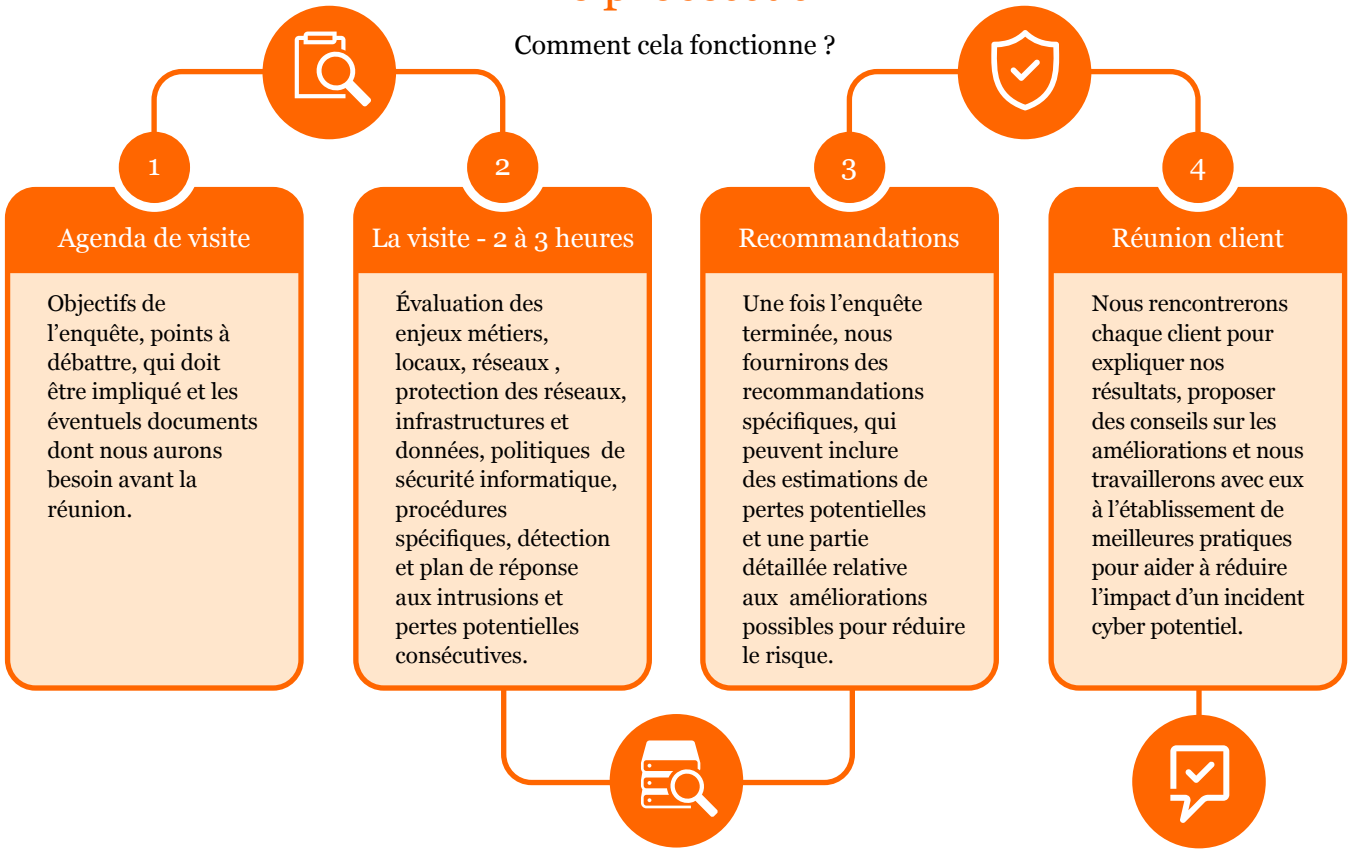
Principaux avantages

- Une intervention directe auprès des clients pour une compréhension approfondie du risque et des expositions
- Intervention de l'assureur avant ou après mise en place de la police
- Recommandations sur la gestion des risques, la façon dont les clients peuvent globalement améliorer la gestion de leurs risques cyber
- Une formation technique complémentaire est disponible pour les clients et courtiers

Même si ce service est au 1er chef destiné aux Grandes Entreprises, il peut être proposé quelle que soit la taille de l'entreprise.

Le processus

Comment cela fonctionne ?



Grandes entreprises - Vue d'ensemble

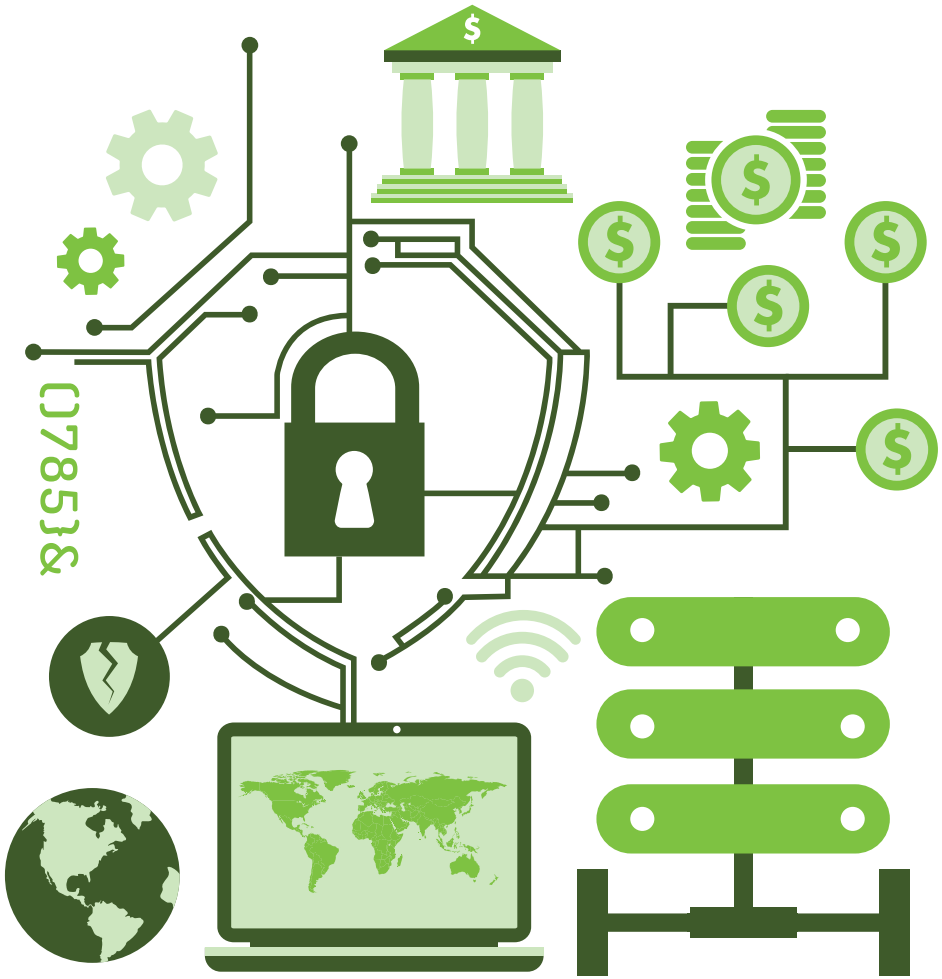
Le nombre de cyberattaques largement médiatisées contre de grandes entreprises ou des multinationales ayant augmenté ces dernières années, la demande d'assurances cyber s'est rapidement intensifiée. Cette demande croissante a été alimentée par une pression accrue sur les conseils d'administration afin que ces derniers montrent qu'ils ont entrepris une évaluation précise des risques cyber, une surveillance plus étroite de la réglementation, et un besoin croissant de communiquer sur ces sujets en interne aussi bien que vis-à-vis des clients et partenaires externes. Les conseils d'administration et les Risk Managers attendent autre chose de leur couverture cyber qu'un simple transfert de risques. L'offre de Chubb pour les grandes entreprises fournit une solution globale, tout en restant flexible, de services de réponses à incident, un large choix d'options pour les multinationales, des possibilités de fronting de captives de réassurance, et des capacités importantes via l'offre 'Global Cyber Facility'.

Services de réponses à incident pour les grandes entreprises

Les plans de réponse à incident cyber sont très souvent mis en place et régulièrement testés par les grandes entreprises. Le service de réponses à incident de Chubb est destiné à compléter les dispositifs déjà en place. Notre équipe de managers des services de réponse à incident est habituée à travailler avec les prestataires spécialisés avec lequel travaille déjà un assuré, même si ceux-ci ne figurent pas dans le panel de Chubb.

- La police inclut le recours à des prestataires avec qui nos clients ont déjà établi un contrat dans le cadre d'un plan de réponse à incident cyber.
- Notre réseau mondial d'équipes locales de réponse à incident est taillé pour répondre aux besoins de gestion des risques cyber des multinationales.
- La Cyber Alert® app de Chubb, conçue pour un Risk Manager ou un responsable informatique, leur permet de contacter notre équipe de réponse à incident et à celle du département indemnisations ce qui simplifie l'intervention des experts et le déploiement du service 'réponse à incident' liée à la police d'assurance.
- « Réponse d'urgence aux incidents » fournit une assistance à la suite d'un incident cyber.

Cliquez ici pour obtenir plus d'informations sur le fonctionnement de la solution de réponse à incident de Chubb.



Grandes entreprises

1 Programmes internationaux

La nature par définition globale des risques cyber a obligé les entreprises à comprendre comment leurs polices d'assurance peuvent jouer suite à un incident transfrontalier, et quelles restrictions pourraient éventuellement s'appliquer dans tel ou tel pays. La structuration d'un programme d'assurance international efficace et rentable exige une compréhension approfondie du cadre réglementaire évolutif concernant la cybersécurité.

Voici quelques questions spécifiques à vous poser lorsque vous envisagez la mise en place d'un programme d'assurance international :

- Où sont situées les entités ? Les règlementations peuvent différer d'un pays à l'autre.
- Les pays autorisent-ils un assureur non agréé à payer des pertes directement à l'entité locale ?
  Quelles sont les règlementations d'un pays spécifique ?
- Le client souhaite-t-il protéger les assurés au niveau local ? Les avantages d'une police locale comprennent : des indemnisations versées au niveau local, une police dans la langue locale et une gestion locale des sinistres.

Compétences de Chubb en matière de programmes cyber internationaux :

Chubb peut proposer des programmes cyber internationaux pour couvrir localement et de façon consistante dans plus de 35 pays dans le monde entier, avec des services fournis par une équipe dédiée et reposant sur l'expertise de spécialistes prêts à répondre aux besoins et apporter une assistance aux Groupes Internationaux.

2 Offre 'Global Cyber Facility'

Une solution complète de gestion des risques cyber pour les grandes entreprises.

Avec qui travaillons-nous ?

- Des entreprises ou institutions réalisant plus de 1 milliard CHF de chiffre d'affaires annuel.
- Tous les secteurs d'activité, notamment les détaillants, institutions financières et le secteur manufacturier.

Composantes de l'offre :

- Services de contrôle des dommages pré-incident de la part de prestataires spécialisés en Cyber Sécurité mondialement reconnus pour répondre aux déficiences de cybersécurité identifiées lors de l'évaluation des risques.
- Une solution de transfert des risques sur mesure.
- Services de réponse à incident et gestion des sinistres.

Principales couvertures de la police :

- Capacités disponibles de 30 M CHF jusqu'à 100 M CHF en première ligne ou concernant des montages en ligne .
- Avenants DIC/DIL disponibles pour combler les insuffisances de garanties entre les polices cyber et les polices Responsabilité Civile ou Dommages d'une entreprise.
- Textes de police sur mesure disponible.

Quel est le processus ?

- Commencer de manière proactive le processus de vente trois mois avant l'offre sur le marché.
- Évaluation interne de Chubb en matière d' analyse du profil de risques de l'entreprise.
- Implication directe avec le client et le souscripteur Chubb (ingénierie des risques également disponible).

Grandes entreprises

3 Captives

La gestion des risques cyber à l'intérieur d'une captive devient de plus en plus pertinent pour les multinationales qui trouvent intéressante la combinaison de transfert de risques et de conservation des risques. Le recours aux captives pour l'assurance des risques cyber est en train de devenir une solution courante, soit pour maintenir un niveau de prime acceptable, ou pour gérer de manière optimale les différents niveaux de franchises des polices locales.

Une captive peut également fournir une couverture plus complète que ce qui est disponible sur le marché. Cela permet à une entreprise d'obtenir une meilleure compréhension des risques cyber, de suivre l'historique sinistres, permettant ainsi d'optimiser les conditions d'intervention de l'assureur ou du réassureur.

Pourquoi

- Optimiser le transfert de risques
- Assurer une forme de diversification
- Agir comme incubateur
- Accès à des services complémentaires

Comment

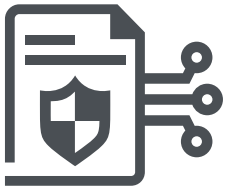
- Plusieurs structures possibles
- 1ère ligne d'un faible montant/franchise élevée
- Quote-part de programmes importants
- Fait générateur spécifique

Défis

- Compréhension de l'exposition / risque d'occurrence
- Tarification de la rétention
- Agrégation avec d'autres lignes

Principaux arguments de vente

Certains de vos clients ne saisiront pas l'importance d'une police d'assurance cyber, ni tous les avantages qu'elle peut fournir. Nous avons rassemblé quelques éléments clés à connaître pour vous aider à expliquer ces principaux avantages à vos clients.



Protection dédiée

Les polices d'assurance traditionnelles peuvent ne pas être adaptées pour répondre aux expositions cyber. Une police cyber est conçue précisément pour remédier à ces insuffisances de garantie et vous fournir une protection effective face à une exposition qui peut être difficile à définir.

Il n'est pas nécessaire d'être la cible pour être affecté

Les cyberattaques peuvent vous atteindre à travers vos fournisseurs ou prestataires externes de technologie, conduisant à un impact financier significatif alors même que vous n'êtes pas directement ciblés. Chubb a géré des dommages collatéraux importants lors d'incidents cyber ayant débuté dans des entreprises sans lien entre elles. Et si votre fournisseur de services informatiques / stockage de données était ciblé, et que vos données étaient ainsi compromises ?

L'assurance couvre les frais de réponse à incident et les frais de rétablissement, et pas seulement les conséquences d'une compromission de données

La responsabilité civile engendrée par la perte ou l'utilisation frauduleuse de données sensibles n'est qu'une des conséquences potentielles d'un incident cyber. Les pertes d'exploitation, les frais de réponse à incident et les frais de remise en état représentent une part importante des indemnisations versées par Chubb, même en l'absence de réclamation d'un tiers.

Complément aux équipes informatiques déjà en place

L'assurance cyber n'interfère en aucun cas sur l'efficacité des équipes de sécurité informatique : elle apporte une protection complémentaire en protégeant l'entreprise d'un incident difficilement prévisible.

Principaux arguments de vente

Menaces internationales

Les dommages cyber ne sont pas cantonnés aux États-Unis. Chubb aide des entreprises à se remettre d'incidents cyber partout dans le monde, notamment là où nous observons plus particulièrement des violations de données, des attaques par rançongiciel et d'autres incidents.

Toutes les entreprises peuvent être touchées

Les incidents cyber peuvent affecter toute entreprise, quelle que soit sa taille ou son secteur d'activité. Les incidents peuvent être ciblés, les employés peuvent faire des erreurs ou des pertes dues à des dommages collatéraux peuvent survenir à la suite d'un incident plus important. Chubb propose des solutions adaptées à vos besoins, à votre niveau de maturité ou à la taille de votre entreprise.

Une réponse à une réglementation en évolution

Les nouvelles réglementations en matière de protection de la vie privée intègrent des normes et imposent des sanctions de plus en plus élevées. L'assurance cyber peut vous aider à faire face à ces changements. La police d'assurance de Chubb s'adapte à ces réglementations.

S'adapter à des risques cyber émergents

Chubb fournit des tendances de sinistres cyber sur une base trimestrielle, vous tenant ainsi informés des nouveaux risques dès que nous les observons. Le Cyber Index℠ de Chubb vous offre également des informations à jour sur les tendances récentes ou observées il y a plus longtemps.

Hacksagon !

Avez-vous joué au jeu de société cyber de Chubb, Hacksagon ! ? C'est un excellent outil de vente et de formation pour aider les clients à mieux comprendre les menaces cyber et la réponse de l'entreprise. Contactez votre souscripteur local pour plus d'informations.

Services de prévention des risques

Notre suivi permanent de la sinistralité met en lumière de grandes tendances propres à tel ou tel secteur d'activité. L'erreur humaine, l'utilisation frauduleuse et les attaques par ingénierie sociale comme l'hameçonnage sont des causes habituelles de dommages cyber mais on peut les éviter ou les réduire à travers des programmes de sensibilisation et/ou de formation adaptés.

Dans le cadre de la solution d'assurance cyber de Chubb, nous proposons des services de prévention des risques spécialement conçus pour réduire le risque d'occurrence d'un dommage cyber. Les assurés Chubb ont accès à un grand nombre de services, notamment relatifs à la sécurité des mots de passe, la formation sur l'hameçonnage, la sensibilisation des employés, et plus encore.

Notre philosophie d'entreprise au sujet de la gestion des risques montre notre fort engagement à améliorer la gestion des risques cyber chez nos clients. En développant des partenariats avec des prestataires experts, nous fournissons à nos clients un accès à des services d'amélioration simples à mettre en place pour mieux maîtriser les risques cyber, dont un grand nombre sont gratuits.

Pour vous inscrire aux services et pour obtenir plus d'informations, veuillez visiter le site Chubb Cyber Services :

www.chubb.com/cyber-services

Services de prévention des risques

1. Gestion des mots de passe de Dashlane

Une gestion de mots de passe robustes est la base d'une bonne politique de sécurité L'historique des sinistres gérés par Chubb montre qu'une gestion insuffisante des mots de passe peut conduire à des dommages cyber importants. L'outil de gestion de mots de passe de Dashlane est offert à tous les assurés cyber de Chubb.

2. Évaluation de la sensibilisation au hameçonnage par Cofense

Ce programme de formation sur l'hameçonnage est destiné à identifier la possibilité et le risque d'une attaque par hameçonnage, un risque qui peut provoquer de nombreux incidents cyber.

3. L'appli Cyber Alert® de Chubb

Répondre à un incident cyber peut s'avérer très compliqué, et les coûts de gestion d'incident peuvent augmenter s'il n'est pas fait appel à l'assistance d'un expert spécialisé. L'application gratuite Cyber Alert® de Chubb offre aux assurés un moyen efficace et immédiat pour signaler un incident et se mettre en relation avec des spécialistes du panel d'intervention.

4. Autres services

Des formations sur la cybersécurité, des évaluations de risques, des exercices de planification et d'autres services de prévention des risques sont disponibles pour les assurés dans certains pays. Découvrez ce qui est disponible dans votre pays ici :

www.chubb.com/uk-en/business/cyber-services-registration.aspx

Informez-vous sur les services de réponse à incident lorsque l'incident ne peut être évité.

En savoir plus

Services de réponse à incident - Vue d'ensemble

Même si les services de prévention des risques de Chubb peuvent aider à réduire la probabilité d'un incident cyber, la réalité est qu'aucun niveau de protection n'est infaillible contre les menaces de cybersécurité. Les polices cyber de Chubb incluent l'accès au panel de spécialistes de l'équipe d'intervention 24h/24, 7j/7 et 365j/an. L'équipe d'intervention est mise en place pour aider nos assurés à se remettre d'un incident cyber.

Faits marquants

Chubb aide trois à cinq entreprises par jour à se remettre d'un incident cyber dans le monde.

Lorsque des assurés notifient un incident cyber via le centre de réponse à incident cyber de Chubb, ils reçoivent une assistance immédiate de la part d'un spécialiste de l'équipe d'intervention pour recueillir les premiers éléments de l'incident afin de faire intervenir les bons experts. Dans 90 % des cas, nos assurés sont rappelés dans les 15 minutes.

Recours possible à des prestataires autres que ceux du panel – nous sommes conscients que certaines entreprises souhaiteront faire appel à des prestataires qui ne font pas partie de notre réseau. Chubb offre une flexibilité aux assurés concernant le choix des prestataires dans de nombreux pays, et ceux-ci peuvent être intégrés sans difficulté dans notre réseau de réponse à incident.

Voyez comment notre processus de réponse à incident fonctionne ici :

Suivant

Services de réponse à incident - Fonctionnement

Ce guide explique en détail comment contacter l'équipe de réponse à incident cyber Chubb, comment déclarer un sinistre et qu'attendre de la plateforme de réponse à incident.

1 Le client est victime d'un incident cyber

La plateforme de réponse à incident Chubb est disponible 24h/24, 7j/7 et 365j/an. Elle donne accès au centre d'appel du service d'assistance et à notre panel de spécialistes de l'équipe d'intervention et propose une approche globale de la gestion des incidents cyber.

2 Le client signale l'incident cyber en utilisant l'un des moyens suivants :

L'application mobile Chubb Cyber Alert®

Vous la trouverez sur l'Apple Store et le Google Play Store

Le site web Chubb Cyber Alert

Accédez à notre plateforme www.chubbcyberalert.com

La ligne d'urgence Chubb Cyber Alert

Vous trouverez votre numéro local ci-dessous :

Numéros d'appel locaux gratuits

Argentine	800 666 1967
Australie	1 800 027428
Autriche	0800 005 376
Belgique	800 49 405
Brésil	0800 095 7346
Canada	1 866 561 8612
Chili	1 230 020 1212
Chine	400 120 5310
Colombie	01 800 518 2642
République Tchèque	800 142 853
Danemark	80 250 571
Finlande	0 800 1 12382
France	08 05 10 12 80
Allemagne	0800 589 3743
Hong Kong	800 900 659
Indonésie	001 803 011 2974
Irlande	1 80 093 7331
Israël	1 80 921 3812
Italie	80 019 4721
Japon	00531 1 21575
Corée du Sud	00798 14 800 6017
Malaisie	1 800 8 12541
Mexique	001 855 250 4580
Pays-Bas	0800 020 3267
Nouvelle-Zélande	0800 441402
Norvège	800 12554
Panama	001 800 507 3360
Pérou	0800 56006
Pologne	00 800 121 4960
Portugal	800 8 14130
Singapour	800 120 6727
Afriquedu Sud	080 09 82340
Espagne	800 810 089
Suède	020 088 3181
Suisse	080 016 6223
Taïwan	00801 13 6828
Turquie	0811 213 0171 (ligne fixe)
Turquie	0812 213 0043 (ligne mobile)
Émirats Arabes Unis	8000 444 4411
Royaume-Uni	0800 279 7004
États-Unis	1 844 740 9227
Vietnam	1203 2353 (VNPT)
Vietnam	1228 0688 (Viettel)

Services de réponse aux incidents - Fonctionnement

3 Contact de la part du centre d'appel du service d'assistance de Chubb

Dans la minute suivant le signalement de l'incident, le client sera mis en relation avec un consultant pour la collecte des informations suivantes :

- Nom de l'assuré
- Lieu d'émission de la police d'assurance (Master)
- Coordonnées
- Lieu de l'incident

Des informations seront envoyées à la direction locale de l'équipe d'interventionet peuvent être envoyées au service des déclarations de sinistres de Chubb (selon la décision de l'assuré). Le fait de prévoir la notification de l'incident à Chubb lors du contact avec le centre d'appel permettra la prise en charge des frais de réponse à incident.

4 Gestion des réponses à incident

Dans l'heure suivant le signalement, le client recevra un appel téléphonique de la part d'un coordinateur de l'équipe d'intervention. Les étapes suivantes incluent :

- Conduite de l'investigation initiale
- Développement du plan d'action pour contenir l'incident
- Désignation de spécialistes pour aider en matière de conseil et de récupération :

Investigations informatiques (enquêtes forensiques) | Conseil juridique | Relations publiques | Conformité à la réglementation | Protection contre l'usurpation d'identité | Surveillance de l'utilisation frauduleuse de moyens de paiements | Expertise informatique judiciaire

5 Reprise de l'activité

Grâce à un panel de spécialistes travaillant à limiter les impacts de l'incident, l'équipe de réponse à incident cyber assistera l'assuré dans la reprise de ses activités commerciales.

6 Suivi de l'incident

Les prestataires de l'équipe d'intervention de Chubb discuteront ensuite de l'apport de services additionnels pour aider l'assuré dans l'analyse de l'incident afin d'inclure des mesures correctives, de tirer des leçons du passé et de conseiller sur l'aspect prévention des risques..

Contrat Cyber ERM - Gestion des risques cyber pour les entreprises (Version 2)

La couverture

Garanties Pertes Pécuniaires

- Réponse à incident – suite à un évènement cyber– sans franchise pour les PME et ETI
- Pertes d'exploitation – perte de marge brute
- Rétablissement du système informatique – frais de reconstitution de données et frais supplémentaires d'exploitation
- Cyber extorsion – remboursement des rançons et des frais de cyber extorsion

Tiers

- Responsabilité Civile de l'Assuré en cas d'Atteinte à la confidentialité des données ou à la sécurisation des réseaux responsabilité civile suite à une fuite de données ou une atteinte à la sécurisation des réseaux :
  - Pertes liées aux cartes de paiement Amendes forfaitaires et pénalités PCI DSS
  - Fonds de recours des consommateurs
  - Sanctions administratives (lorsque cela peut être légalement assuré) - RGPD
- Responsabilité civile médias – responsabilité civile suite à une diffamation ou à une atteinte médiatique

Les points principaux

- Carence de fournisseur pour des prestataires de services informatiques extérieurs
- Panne système Faits générateurs : erreur humaine, erreur de programmation, panne de courant, surtension ou diminution d'un système électrique sous le contrôle de l'assuré
- Extensions standards :
  - Frais d'urgence dans les 48 heures pour les Grandes Entreprises– sans franchise
  - Frais d'amélioration – amélioration des logiciels et applications par des versions nouvelles
  - Fraude informatique – perte financière directe suite à un détournement cyber
  - Récompenses
  - Fraude téléphonique
- Paiement pour le compte de l'Assuré des frais de réponse à incidents
- Recours possible à des prestataires de réponse à incident autres que les prestataire prévu par le coordinateur
- Malveillance interne
- Notification volontaire
- Interruption volontaire
- Par avenant : Atteinte à la réputation, Fraude par ingénierie sociale
- Cyber terrorisme
- Programmes internationaux

Appétits

Pour vous offrir plus de clarté ainsi qu'à vos clients, nous avons créé un résumé de nos appétits de souscription. Il ne s'agit pas d'une liste exhaustive mais elle indique les grandes tendances Pour des risques spécifiques ou des secteurs ne figurant pas dans cette liste, contactez notre équipe de souscription pour traiter votre demande.

Privilégiés

- Publicité*
- Agriculture
- Architectes et ingénieurs
- Galeries d'art et musées
- Concessionnaires automobiles et stations-service
- Produits chimiques et dérivés
- Communications*
- Construction
- Ingénierie et gestion/ services dans le secteur industriel
- Gouvernement
- Production/ fabrication alimentaire
- Fabrication industrielle
- Association à but non lucratif
- Impression et publication*
- Fabrication de produits
- Administration publique
- Immobilier
- Etablissements scolaires
- Production TV/ Radio/Cinéma*
- Grossistes-Marchands

Acceptés

- Comptables
- Professionnels paramédicaux
- Gestionnaires d'actifs
- Services de facturation
- Universités et établissements d'enseignement secondaire
- Matériels et logiciels informatiques
- Cabinets médicaux/ dentaires
- Agence pour l'emploi/agence de recrutement
- Entreprise générale de bâtiment
- Cabinets d'avocats -
- Pour entreprises
- Consultants en gestion
- Consultants en marketing
- Exploitation minière
- Courtiers en prêts immobiliers
- Arts du spectacle*
- Services aux particuliers
- Services aux professionnels – Non listés ailleurs
- Consultants techniques
- Associations professionnelles
- Services de transport – Non listés ailleurs

Sélectifs

- Résidences médicalisées (EHPAD)
- Diffusion audiovisuelle*
- Centres d'appel
- Agences de recouvrement
- Traders de matières premières
- Échanges de devises
- Établissements de dépôt
- Institutions financières - Non listées ailleurs
- Hôpitaux
- Assurances - Autres que pour les particuliers
- Gestionnaires de fonds
- Notaires
- Maison de retraite/ repos
- Administrations
- Restaurants/ Hôtellerie
- Vente au détail
- Banque commerciale
- Courtiers en titres et valeurs mobilières
- Télécommunications
- Services de télémarketing*
- Agents de titres
- Services publics

Opportunités

- Casinos
- Infrastructures critiques
- Traitement de données
- Marketing direct*
- Stockage de dossiers médicaux électroniques (DME)
- Entreprises d'affacturage
- Organismes de santé
- Compagnies d'assurance - Assurances de particuliers
- Plateformes de jeux en ligne
- Plateforme de streaming en ligne*
- Prestataires de services de paiement
- Services de paie

Interdits de souscription

- Contenus pour adultes
- Compagnie aérienne
- Échanges de crypto-monnaies
- Création de crypto-monnaie
- Agrégateurs de données
- Enchères en ligne
- Réseaux sociaux
- Plateformes de trading

*N'inclut pas les couvertures Media E&O

CHUBB®

Pour plus d’informations

Veuillez contacter nos souscripteurs pour en savoir plus sur nos offres cyber ou cliquez sur www.chubb.com

Retourner au début