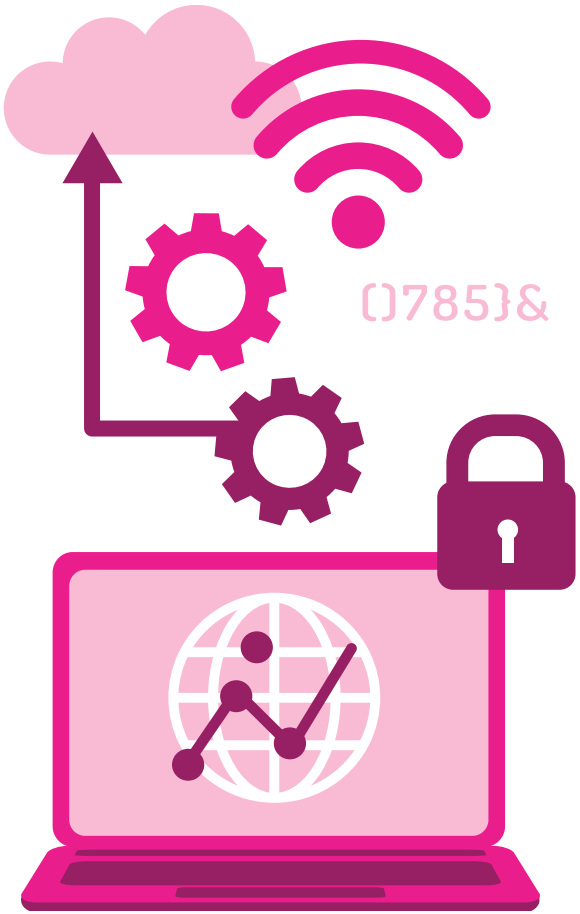
CHUBB®

# Guide de gestion des cyberrisques à l'intention de nos agents et courtiers

# Ce guide contient de l'information sur ce qui suit :

# Pourquoi la cybersécurité est-elle importante?



## L'ère de l'information et du numérique nous permet de recueillir plus de données, de collaborer plus efficacement, de rationaliser les processus commerciaux et d'extraire des informations à l'échelle mondiale en tout temps.

**Une dépendance accrue envers les systèmes informatiques et l'accès à l'information peut accroître considérablement l'exposition d'une entreprise aux menaces de cybersécurité.** Les pannes, les erreurs ou les attaques dont sont victimes ces nouveaux processus peuvent entraîner des dépenses supplémentaires qui peuvent avoir des conséquences désastreuses sur les résultats de l'entreprise. Lorsque cela se produit, vous avez besoin d'une protection élargie d'un assureur qui se spécialise dans la gestion des cyberrisques, offre un éventail complet de solutions d'assurance intégrées afin d'aider à atténuer les lacunes dans la couverture, et comprend comment adapter la protection à votre entreprise. **Chubb offre des solutions en cyberrisques à ses assurés depuis 1998.**

### Lacunes de l'assurance traditionnelle

Des entreprises peuvent estimer que leurs polices d'assurance actuelles sont suffisantes pour couvrir les risques en matière de sécurité des données et de respect de la vie privée auxquels elles sont exposées. Ce n'est malheureusement pas toujours le cas et les polices d'assurance traditionnelles peuvent ne pas répondre adéquatement aux risques auxquels les entreprises sont exposées aujourd'hui. Examinons les polices traditionnelles suivantes :

| Responsabilité civile générale | Assurance des biens | Assurance contre les vols et les détournements |
|---|---|---|
| Les polices d'assurance responsabilité civile générale sont habituellement utilisées en réponse à des réclamations pour dommages corporels (DC) et pour dommages matériels (DM). Les cyberévénements n'impliquent habituellement pas de DC ni de DM et les polices d'assurance responsabilité civile générale n'offrent habituellement pas de couverture des risques propres. | Les polices d'assurance des biens interviennent habituellement à la suite de la destruction ou de l'endommagement de biens matériels découlant d'un risque physique. La perte matérielle permet alors à la garantie en cas d'interruption des activités et de frais supplémentaires de couvrir les pertes. Un cyber-événement, en soi, peut ne pas causer de dommage matériel, mais tout de même entraîner la fermeture d'une entreprise, ce qui se traduit par des frais substantiels et une perte de revenu. | Les polices d'assurance contre les vols et les détournements couvrent habituellement les sinistres directs causés par le vol d'argent, de valeurs mobilières ou de biens matériels par des employés. Les extensions de couverture pour crime informatique excluent habituellement la responsabilité civile vis-à-vis de tiers et peuvent ne pas couvrir suffisamment la perte de renseignements confidentiels. |

# Expositions par secteur

## Institutions financières

Les institutions financières sont fortement exposées au cyberrisque en raison d'un ensemble de facteurs. La cybercriminalité, le cybermilitantisme et les pirates aguerris faisant de l'espionnage pour un bénéficiaire ne représentent que certains des risques dont il faut tenir compte. Les vulnérabilités aux cyberévénements peuvent être grandes puisque de nombreuses institutions financières dépendent de réseaux et d'infrastructures essentielles hautement interconnectés. Comme elles dépendent fortement de la technologie, la plupart des institutions financières seront de plus en plus exposées aux cyberrisques.

Réclamations courantes : **social – hameçonnage** et **erreur humaine**

## Soins de santé

Un vaste mouvement de numérisation des dossiers médicaux a créé chez les sociétés du secteur des soins de santé une dépendance accrue envers les systèmes informatiques pour la collecte et le traitement des données médicales personnelles très sensibles. Le fait de compter sur des employés pour entrer des informations exactes dans les systèmes entraîne un risque élevé d'erreurs administratives. Souvent, les anciens systèmes informatiques côtoient les nouveaux, ce qui accroît le potentiel qu'un événement ait une incidence majeure sur les activités.

Réclamations courantes : **erreur humaine** et **mauvaise utilisation**

## Vente au détail

Qu'il s'agisse de commerces en ligne ou de magasins physiques, les données sur les réclamations de Chubb indiquent que le secteur de la vente au détail est considérablement exposé aux cyberpertes. Les entreprises de détail comptent souvent de nombreux établissements qui peuvent utiliser ou non des systèmes informatiques centralisés, dépendent des réseaux complexes de fournisseurs de services informatiques essentiels et dépendent possiblement de sites Web pour traiter le nombre croissant de ventes en ligne et de renseignements personnels sensibles agrégés compte tenu de la fréquence élevée de transactions financières et du grand nombre de programmes de fidélité.

Réclamations courantes : **piratage** et **social – hameçonnage**

## Hôtellerie

Le secteur de l'hôtellerie couvre un vaste éventail d'activités allant des hôtels aux bars en passant par les restaurants. Dans ce secteur, les expositions aux cyberrisques sont notamment liées aux volumes élevés de renseignements sur les clients et les employés, ainsi qu'à l'utilisation intensive de sites Web pour les réservations des clients et le traitement des informations des programmes de fidélité qui peuvent occasionner des problèmes de protection de la vie privée, puisque ces informations peuvent être la cible d'attaques par piratage psychologique et d'hameçonnage.

Réclamations courantes : **social – hameçonnage** et **piratage**

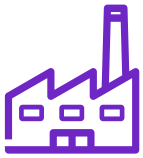
## Services professionnels

Compte tenu de la quantité de données confidentielles recueillies, le secteur des services professionnels constitue une cible de prédilection pour les cyberattaques. Par exemple, les renseignements et les fonds détenus par un cabinet juridique ou comptable peuvent être payants pour un cybercriminel, et les conséquences pour la réputation d'un cabinet ayant été victime d'une violation peuvent causer beaucoup de dommages. L'agrégation de données sensibles sur les clients a alimenté une hausse des cyberévénements ayant une incidence sur les cabinets de services professionnels au cours des dernières années.

Réclamations courantes : **erreur humaine** et **piratage**

* Les causes courantes de réclamations en matière de cyberrisques sont tirées du Chubb Cyber Index®.

# Expositions par secteur



## Fabrication

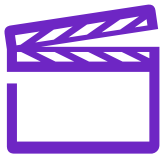
La fabrication est l'un des plus grands secteurs ciblés par les cybercriminels. L'intégration importante des technologies change la façon dont les fabricants exploitent leurs entreprises. Pour améliorer leur productivité et leur rentabilité, de nombreux fabricants misent sur l'Internet des objets (IDO), la numérisation et les services infonuagiques, qui augmentent tous l'incidence de certains cyberévénements. Les événements récents touchant des systèmes de contrôle industriel (SCI) et des systèmes de télésurveillance et d'acquisition de données (SCADA) ont eu un effet désastreux sur les activités de certaines entreprises.

Réclamations courantes : **logiciel malveillant** et **social – hameçonnage**

## Éducation

Les établissements d'enseignement sont à risque en raison des données sensibles qu'ils détiennent sur leurs étudiants et leur personnel. Les écoles et les universités ont souvent des budgets et des ressources limités à consacrer aux TI. Les menaces sont à la fois externes et internes, qu'elles proviennent d'un étudiant introduisant un logiciel malveillant dans le réseau intentionnellement ou par inadvertance, ou d'un membre du personnel qui ne suit pas le protocole et cause une atteinte à la protection des données.

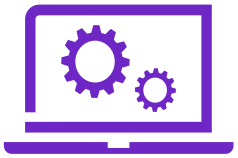
Réclamations courantes : **social – hameçonnage** et **piratage**



## Médias/Divertissement

Les entreprises du secteur des médias et du divertissement reçoivent souvent des menaces d'extorsion qui peuvent cibler par matériel et du contenu sensibles. Les attaques par déni de service distribué (DDoS) ou les pannes de systèmes informatiques peuvent avoir une incidence importante sur les activités de transmission et sur la diffusion de contenu en temps voulu. Le fait de détenir des renseignements personnels sensibles sur les abonnés aggrave l'exposition au risque.

Réclamations courantes : **erreur humaine** et **social – hameçonnage**



## Technologie

Les entreprises technologiques ont la confiance de leurs clients, qui les voient comme des chefs de file de l'industrie en matière de cybersécurité et de protection des données, ce qui accroît l'atteinte à la réputation qui pourrait suivre un cyberévénement. Les cyberévénements subis par des fournisseurs de services technologiques peuvent également avoir une incidence sur les garanties d'assurance erreurs et omissions technologiques – veuillez communiquer avec votre souscripteur chez Chubb pour obtenir de plus amples renseignements sur notre offre combinée d'assurance erreurs et omissions technologiques et contre les cyberrisques.

Réclamations courantes : **piratage** et **erreur humaine**

* Les causes courantes de réclamations en matière de cyberrisques sont tirées du Chubb Cyber Index®.

**Voyez ce que Chubb peut offrir aux petites, moyennes et grandes entreprises pour couvrir ces risques :**

Petites entreprises

Marché intermédiaire

Grandes entreprises

# Petites entreprises – Aperçu

Les cyberévénements touchant les grandes organisations reçoivent davantage d'attention médiatique, mais les petites et moyennes entreprises (PME) sont souvent touchées par des cybermenaces et des vulnérabilités cybernétiques. Les petites entreprises sont souvent perçues comme des cibles plus faciles pour les cybercriminels, car elles ont souvent des ressources et des investissements limités à consacrer aux TI.

Par ailleurs, elles sont moins susceptibles d'avoir investi dans des mesures telles que la formation du personnel sur la sécurité des données, des conseils sur la configuration des mots de passe et l'authentification à deux facteurs. Les PME représentent souvent un créneau payant pour les cybercriminels comparativement aux plus grandes organisations chez lesquelles il peut être plus difficile de trouver des failles. Elles doivent aussi tenir compte du fait qu'elles peuvent ne pas être la cible initiale, mais peuvent simplement être touchées par un événement subi par un fournisseur de services informatiques impartis ou par un partenaire commercial.

## Réclamations de petites entreprises – Chubb Cyber Index®

Les données sont le meilleur outil pour illustrer les cyberrisques auxquels les petites entreprises sont exposées. Chubb traite des réclamations en matière de cyberrisques depuis plus de deux décennies. Dans le cadre du processus de réclamation, nous surveillons les indicateurs clés, comme les actions ayant causé une cyberperte, qu'un cyberévénement ait été causé par un intervenant interne ou externe, le nombre de dossiers touchés, ainsi que la taille et le secteur de l'assuré touché. Nous partageons ces données publiquement dans le Chubb Cyber Index®, pour aider les entreprises à mieux comprendre les risques auxquels elles sont exposées.

Le Chubb Cyber Index® donne aux utilisateurs un moyen de cerner les principaux cyberrisques auxquels leur entreprise peut être exposée à partir d'exemples concrets d'atteinte à la protection des données. Les utilisateurs peuvent définir des paramètres pour voir des tendances historiques selon le type de menace, la taille d'une société et le type de secteur d'activité de la société.

Pour obtenir de plus amples renseignements, veuillez consulter le Chubb Cyber Index® à l'adresse suivante : **https://chubbcyberindex.com.**

# Petites entreprises – Scénarios de réclamations

## Rançongiciel

Notre assuré, une entreprise de construction, a été victime d'une attaque par rançongiciel ciblée. Les systèmes de l'assuré ont subi une intrusion après qu'un employé a cliqué sur un lien malveillant dans un courriel. Les systèmes et les serveurs de l'assuré ont été cryptés, puis l'assuré a reçu une demande de rançon de 900 000 $ en bitcoins. L'assuré a fait appel à des experts-conseils en intervention en cas de cyberincident pour charger le service d'informatique judiciaire d'établir la méthode et l'étendue de l'attaque. L'entreprise n'a pas payé la rançon, mais toutes ses activités ont été perturbées pendant plus de six mois.

### Atténuation

Des examens réguliers de la sécurité informatique, la formation des employés, des sauvegardes régulières des données et l'établissement d'un plan de reprise après sinistre et d'un plan de continuité des activités sont des mesures à prendre pour aider à atténuer les risques.

## Employé mécontent

Notre assuré a été victime d'un employé sans scrupules qui a volé les fiches de données personnelles de plus de 700 clients contenant leurs noms, leurs adresses et leurs numéros de téléphone. L'employé a transmis ces fiches à son nouvel employeur afin que celui-ci en tire des avantages. Comme cet événement s'est produit après l'adoption du RGPD, un avis a été donné au bureau de l'autorité de réglementation locale et aux parties touchées.

### Atténuation

Il est extrêmement difficile d'empêcher des employés sans scrupules de chercher à causer des dommages. Dans la majorité des cas, ils ont accès au système requis pour pouvoir voler des données personnelles ou d'entreprise sensibles. Une solution d'assurance contre les cyberrisques de Chubb offre les outils nécessaires pour réagir lorsqu'un tel événement se produit.

## Erreur d'un employé

Notre assuré, une association d'habitation, a subi par inadvertance une atteinte à la protection des données découlant de l'erreur d'un employé. En publiant une nouvelle annonce au sujet d'un immeuble vacant, l'employé a inclus par erreur une image des dossiers d'un autre client dans la brochure sur l'immeuble en ligne.

### Atténuation

Il est important de mettre en place une politique de confidentialité à l'échelle de l'entreprise déterminant de manière détaillée le protocole de traitement des données sensibles. Les employés devraient être tenus de comprendre la politique et d'attester leur conformité à celle-ci au moins une fois par année.

# Petites entreprises – Scénarios de réclamations

## Accès non autorisé – Hameçonnage

Notre assuré, une société de logistique, a été victime d'une attaque d'hameçonnage par logiciel malveillant. Une fenêtre intruse est apparue sur l'ordinateur d'une employée de l'équipe de RH de l'assuré après que celle-ci a cliqué sur un lien malveillant reçu par courriel. La fenêtre disait que l'ordinateur était infecté et qu'elle devait appeler au numéro indiqué. Des fraudeurs ont alors eu accès à l'ordinateur de l'employée à distance en la leurrant davantage au cours de l'appel.

### Atténuation

Même si l'entreprise dispose de la meilleure technologie et des meilleurs systèmes de sécurité, le personnel demeure souvent la ressource la plus vulnérable d'un assuré. Le personnel peut se laisser convaincre de donner ses mots de passe ou de permettre l'accès à des données sensibles. Il est recommandé de donner des formations régulières sur l'hameçonnage et il est essentiel de souscrire une police d'assurance permettant de transférer les risques.

## Perte de dossiers physiques de données

Notre assuré, un cabinet d'avocats, a appelé la ligne d'assistance de l'équipe d'intervention en cas d'incident de Chubb lorsqu'il est apparu qu'un employé du cabinet avait enfreint le protocole du cabinet en sortant des dossiers de clients du bureau et en les laissant dans son véhicule. Le véhicule a par la suite été volé et les dossiers de clients ont été perdus.

### Atténuation

Mettre en place un processus clair pour le stockage numérique et physique des données. Il est important de sauvegarder régulièrement les données, car cela permet de les récupérer rapidement. Adopter une politique de confidentialité à l'échelle de l'entreprise que les employés sont tenus de connaître et de respecter.

# Petites entreprises – Une solution d'assurance contre les cyberrisques que vous pouvez personnaliser et faire évoluer avec vous

## 1 Services d'atténuation des pertes pour les petites entreprises

Pour aider les PME à atténuer les causes courantes de réclamations en matière de cyberrisques, Chubb donne à ses titulaires de police accès à de nombreux services par l'intermédiaire de fournisseurs de services, lorsque la loi le permet.

Des **solutions de gestion des mots de passe** sont offertes pour un maximum de 100 employés par titulaire de police.

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

Des **solutions de gestion des fournisseurs** vous aident à autoriser et à présélectionner des fournisseurs tiers et leurs sous-traitants avant qu'ils intègrent l'écosystème de l'entreprise.

Des **solutions de formation des employés** aident votre équipe à détecter des cybermenaces potentielles, à protéger les données sensibles et à signaler les problèmes aux bonnes personnes, s'il y a lieu.

**Cliquez ici pour de plus amples renseignements sur notre gamme complète de cyberservices, dont la cybersécurité et bien plus encore.**

## 2 Services d'intervention en cas d'incident pour les petites entreprises

Chubb comprend que les événements ne peuvent pas tous être évités. Lorsqu'un événement se produit, nos polices d'assurance contre les cyberrisques mettent un groupe de fournisseurs de services d'experts en intervention en cas d'incident à la disposition des PME qui sont nos clientes.

Ces spécialistes sont disponibles en tout temps et sont prêts à vous aider à vous remettre d'un cyberévénement.

- Ce groupe est composé notamment d'experts spécialisés en gestion des interventions en cas d'incident, en informatique judiciaire, en ressources juridiques et en relations publiques.
- L'accès au réseau du fournisseur est inclus dans la police.
- Accessible en tout temps au moyen de l'application Cyber Alert[MC] ou de la ligne d'assistance sans frais.
- Ces experts peuvent offrir de l'aide à la suite d'un cyber-événement avéré ou suspecté – ils sont là pour apporter leur aide dans toute situation d'urgence.

## 3 Plateformes pour les petites entreprises

Les plateformes en ligne de Chubb (offertes dans certains pays) ont été conçues spécifiquement pour permettre aux courtiers de produire des devis et d'engager des protections d'assurance pour des petites entreprises en ligne. En combinant une conception intuitive et une expérience axée sur le client, les courtiers peuvent planifier l'assurance contre les cyberrisques de leurs clients en quelques minutes avant de produire la documentation sur-le-champ.

**Planification rapide et facile de l'assurance – comporte les mêmes avantages que les polices offertes hors ligne :**

- Questions simples
- Vaste appétit de souscripton pour les PME
- Même libellé pour les polices d'assurance contre les cyberrisques que celui utilisé pour les polices hors ligne
- Accès aux services d'atténuation des cyberpertes de Chubb
- Modification des dates des polices, des limites de garantie, des taux de commission et des coordonnées sans devoir communiquer avec un souscripteur
- Production de devis et engagement de garanties en quelques minutes

**Veuillez communiquer avec votre souscripteur local de Chubb pour savoir où nos services d'assurance contre les cyberrisques ou d'autres solutions simplifiées pour les PME sont offerts.**

# Marché intermédiaire – Aperçu

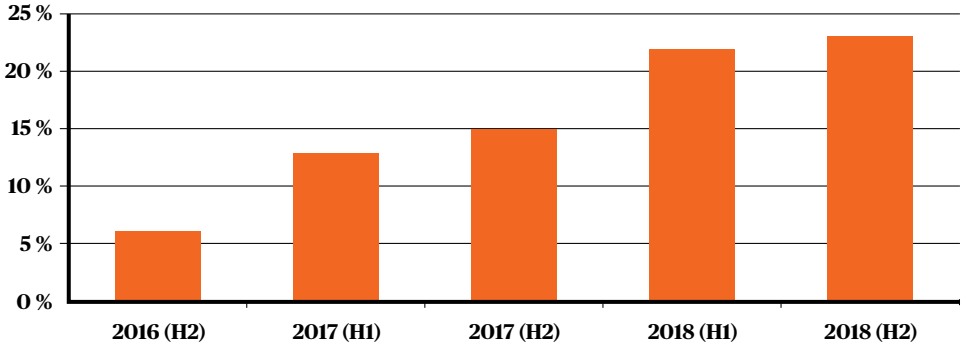
Les entreprises du marché intermédiaire font face aux mêmes problèmes de cybersécurité que les grandes entreprises, mais disposent de budgets moindres et comptent moins de personnel spécialisé pouvant gérer ces risques. Elles ont souvent la même perception que de nombreuses PME clientes et estiment que seules les grandes sociétés d'envergure mondiale sont exposées à des risques importants. Les attaques malveillantes étant devenues plus perfectionnées, le défi auquel font face les entreprises du marché intermédiaire pour se défendre elles-mêmes est plus difficile à surmonter que jamais.

### Chubb Cyber Index®

Le Chubb Cyber Index® donne aux utilisateurs un moyen de cerner les principaux cyberrisques auxquels leur entreprise peut être exposée à partir d'exemples concrets d'atteintes à la protection des données. Les utilisateurs peuvent définir des paramètres pour voir les tendances historiques selon le type de menace, la taille d'une société et le type de secteur d'activité de la société.

Pour obtenir de plus amples renseignements, veuillez consulter le Chubb Cyber Index® à l'adresse suivante : **https://chubbcyberindex.com**.


**Comparaison des réclamations soumises à Chubb et de la 1re moitié de 2016 (croissance en pourcentage)** *Marché intermédiaire – Tous les secteurs*




*H1 = Première moitié de l'année*
*H2 = Deuxième moitié de l'année*

# Marché intermédiaire – Scénarios de réclamations

## Rançongiciel

Une résidence-services a subi une attaque « de force brute » par rançongiciel à l'issue de laquelle plusieurs de ses fichiers ont été cryptés. Une rançon de 25 000 $ environ a été exigée initialement. Après avoir versé une petite partie du montant de la rançon exigée pour obtenir un échantillon de l'outil de décryptage, l'entreprise a plutôt décidé de compter sur ses sauvegardes pour rétablir ses systèmes.

### Atténuation

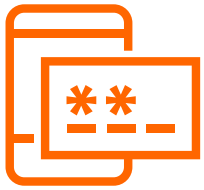
Les technologies de sécurité dans lesquelles les entreprises investissent, bien qu'elles soient essentielles pour aider à prévenir des accès non autorisés, ne sont pas infaillibles. Les cybercriminels perfectionnent constamment leurs méthodes d'attaque, et toutes les entreprises doivent évaluer leur sécurité et leurs procédures régulièrement pour suivre le rythme des menaces.

## Erreur d'un employé

Un employé d'un détaillant en quincaillerie n'a pas tenu compte des politiques et des procédures internes et a ouvert un fichier d'apparence anodine joint à un courriel. Le lendemain, le système de commandes et les caisses enregistreuses de la quincaillerie ont commencé à mal fonctionner et une défaillance du réseau a perturbé les opérations commerciales.

### Atténuation

Des formations régulières pour veiller à ce que le personnel sache quoi rechercher dans les fichiers suspects joints à des courriels et connaisse la procédure à suivre en cas de doute sont essentielles pour aider à atténuer les cyberrisques. De plus, un accès immédiat à un expert-conseil en intervention en cas d'incident permettra de réagir rapidement.



## Atteinte à la protection des données

Le réseau d'un hôtel a été piraté, ce qui a potentiellement compromis tous les dossiers des employés et des clients, dont les renseignements de carte de paiement des clients.

### Atténuation

La sécurité par la détection (*detection awareness security*) est un outil efficace pour combattre le piratage. Elle permet la détection rapide des activités suspectes. Le cryptage des données est également primordial pour faire en sorte que les données touchées puissent être extraites et utilisées facilement.

# Marché intermédiaire – Scénarios de réclamations

## Cryptominage

Une entreprise de fabrication a fait l'objet d'une attaque par rançongiciel qui s'est soldée par le cryptage de plusieurs de ses fichiers. Après avoir communiqué avec Chubb au moyen de la ligne d'assistance de l'équipe d'intervention en cas d'incident accessible en tout temps, l'assuré a consulté un expert-conseil en intervention en cas de cyberincident et des experts en informatique judiciaire de notre groupe d'experts en cyberrisques. Par suite de ces discussions, l'assuré a choisi de ne pas payer la rançon. Cependant, après avoir commencé à travailler à remédier à l'attaque par rançongiciel, le cabinet de services d'informatique judiciaire a découvert que l'assuré avait également été victime de cryptominage. Les pirates avaient installé dans le système de l'assuré un logiciel qui minait des bitcoins. Le cryptominage consiste à utiliser le système informatique d'un tiers pour miner des cryptomonnaies à son insu.

### Atténuation

Il est important que les fabricants évaluent régulièrement la sécurité de leurs systèmes informatiques pour éviter que leur production ne soit affectée par une attaque. Afin d'aider à atténuer les perturbations en cas d'attaque future, la société doit envisager d'élaborer un plan de reprise après sinistre ainsi qu'un plan de continuité des activités. Les technologies de sécurité, bien qu'importantes pour aider à prévenir les accès non autorisés, ne sont pas infaillibles. Les cybercriminels perfectionnent constamment leurs méthodes d'attaque, et toutes les entreprises doivent évaluer leur sécurité et leurs procédures pour suivre le rythme des menaces.

## Le vol de données expose les entreprises à de 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 peut avoir eu accès à des informations sensibles sur ses clients, dont la cible d'acquisition d'une société ouverte et un certain nombre de listes de membres de recours collectifs contenant des informations d'identification personnelles (IIP) sur des plaignants. Le technicien en informatique judiciaire dont le cabinet a retenu les services a déterminé que le logiciel malveillant avait été envoyé à même un courriel qui a échappé aux contrôles de filtrage, et avait dupé un utilisateur qui a cliqué sur un lien malveillant afin que celui-ci s'exécute dans le réseau du cabinet.

### Atténuation

Il est important de former le personnel pour veiller à prévenir l'ouverture de courriels malveillants. En outre, les entreprises devraient pouvoir compter sur un système de sécurité informatique capable de détecter les logiciels malveillants qui pourraient passer à travers les mailles du filet.

# Marché intermédiaire – Une solution en cyberrisques personnalisable qui répond aux besoins de votre entreprise

## 1 Services d'atténuation des pertes pour le marché intermédiaire

Pour aider les entreprises du marché intermédiaire à atténuer les causes courantes de réclamations en matière de cyberrisques, Chubb donne à ses titulaires de police accès à de nombreux services.

Les **solutions de gestion des mots de passe** incluses dans la police sont offertes pour un maximum de 100 employés par titulaire de police.

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

Des **simulations d'hameçonnage aux fins de formation** sont offertes aux titulaires de police.

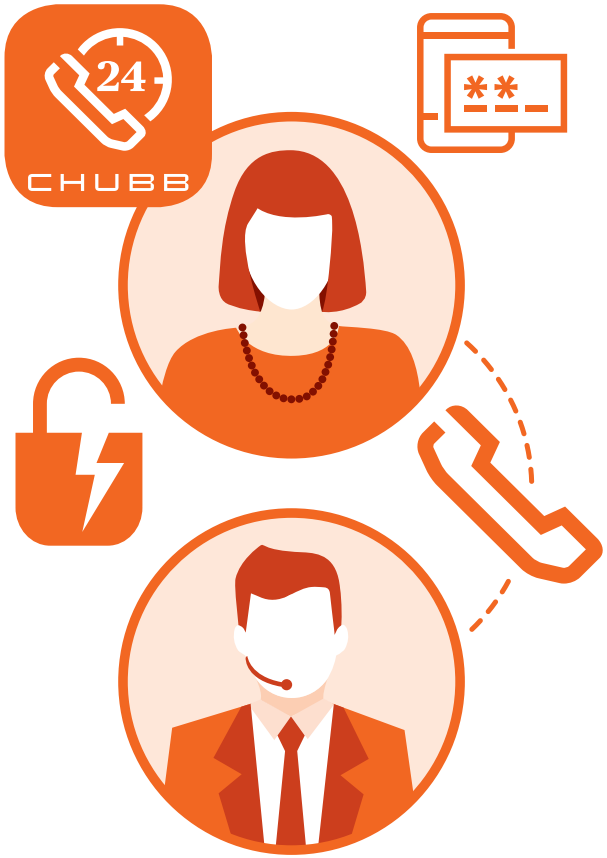
- L'hameçonnage est l'une des causes de cyberpertes évoluant le plus rapidement, et une simple formation offerte aux employés peut être un outil efficace pour freiner une attaque d'hameçonnage visant des entreprises du marché intermédiaire.

**Cliquez ici pour de plus amples renseignements sur notre gamme complète de cyberservices, dont la cybersécurité et bien plus encore.**

## 2 Services d'intervention en cas d'incident pour le marché intermédiaire

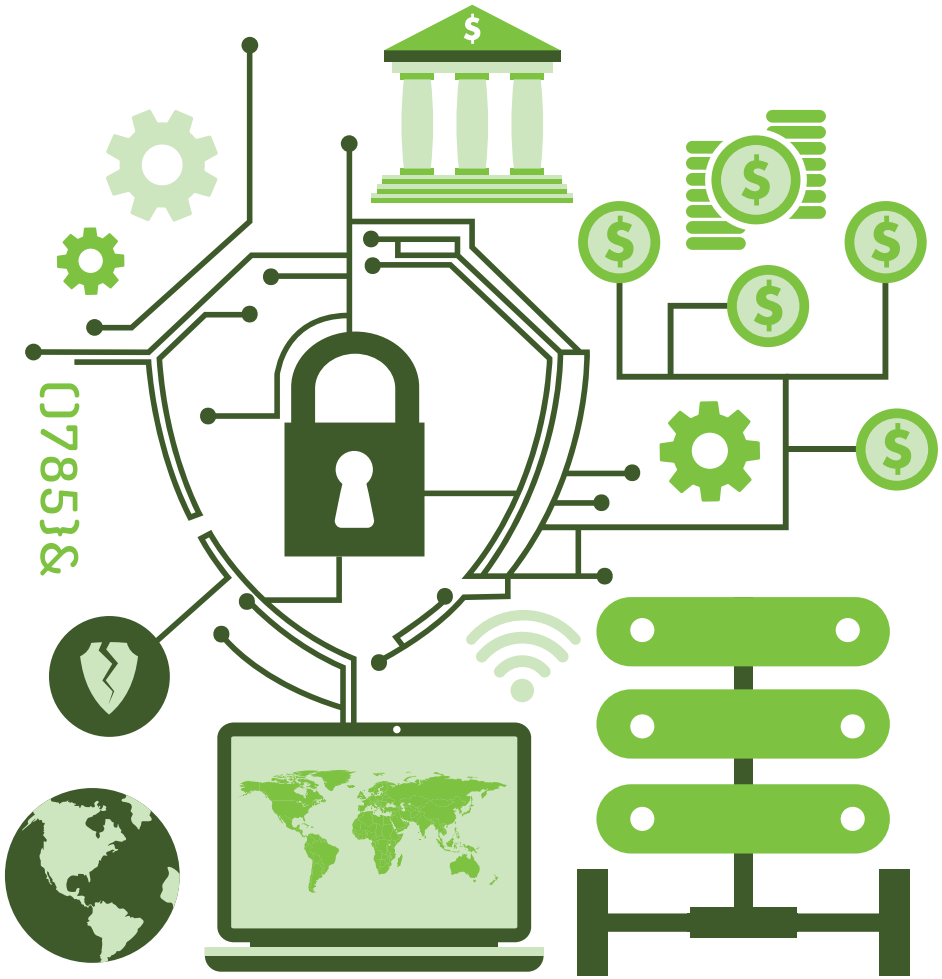
Pour atténuer son incidence et les pertes qu'il occasionne, il est essentiel de répondre rapidement et efficacement à un cyberévénement – dans de telles situations, nos polices d'assurance contre les cyberrisques donnent à nos clients du marché intermédiaire accès à un groupe de fournisseurs de services d'experts en intervention en cas d'incident. Ces spécialistes sont disponibles en tout temps et sont prêts à vous aider à vous remettre d'un cyberévénement.

- Ce groupe est composé notamment d'experts spécialisés en gestion des interventions en cas d'incident, en informatique judiciaire, en ressources juridiques, en relations publiques ainsi que de négociateurs en cyberextorsion.
- Les services offrent la souplesse de faire appel à notre groupe de fournisseurs ou à tout fournisseur avec lequel vous avez déjà conclu un contrat dans le cadre d'un plan d'intervention en cas de cyberincident.
- Offerts en tout temps au moyen de l'application Cyber Alert[MC].



# Grandes entreprises – Aperçu

Comme le nombre de cyberattaques visant de grandes sociétés et des multinationales ayant fait les manchettes a augmenté au cours des dernières années, la demande de produits d'assurance contre les cyberrisques a augmenté rapidement. La demande croissante a été alimentée par l'intensification des pressions exercées sur les conseils d'administration afin que ceux-ci fassent la preuve d'une évaluation précise des cyberrisques, d'une surveillance réglementaire accrue et d'un besoin plus marqué de partage d'information entre collègues et associés. Les conseils d'administration et les gestionnaires de risques sont conscients du fait que l'assurance contre les cyberrisques devrait aller au-delà du transfert des risques. Chubb offre aux grandes entreprises une solution mondiale d'intervention en cas de cyberincident, et néanmoins flexible, de nombreuses options de programmes multinationaux, des capacités d'opérations de façade en assurance captive, et une capacité significative par l'intermédiaire de nos cyberinstallations mondiales.



### Services d'intervention en cas d'incident pour les grandes entreprises

Généralement, les grandes organisations établissent des plans d'intervention en cas de cyberincident et elles les testent fréquemment – les services d'intervention en cas de cyberincident de Chubb visent à compléter ce qui est déjà en place. Notre équipe d'experts-conseils en intervention en cas de cyberincident est prête à travailler avec les fournisseurs spécialisés privilégiés de nos assurés, même s'ils ne font pas partie du groupe d'experts de Chubb.

- Les polices prévoient le recours à des fournisseurs avec lesquels nos clients ont déjà conclu des contrats dans le cadre d'un plan d'intervention en cas de cyberincident.
- Notre réseau mondial d'équipes locales d'intervention en cas d'incident est conçu pour répondre aux besoins de nos clients en matière de risques multinationaux.
- L'application Cyber Alert[MD] de Chubb, conçue pour les gestionnaires de risque et les gestionnaires de TI, met en communication nos équipes d'intervention en cas d'incident et nos équipes responsables des réclamations afin de simplifier l'accès à l'aide d'experts et l'application des polices.

# Grandes entreprises

## 1 Programmes multinationaux

**La nature mondiale des cyberrisques exige que les sociétés comprennent comment leurs polices peuvent s'appliquer en cas d'événement international** et quelles restrictions peuvent s'appliquer. Structurer un programme multinational d'assurance efficace et rentable exige une compréhension approfondie du contexte réglementaire en évolution.

**Certaines questions précises se posent lorsque l'on envisage de créer un programme d'assurance multinational :**

- Où les entités sont-elles situées? Les restrictions peuvent varier d'un pays à l'autre.
- Les pays permettent-ils aux assureurs non agréés de verser une indemnité pour les pertes directement à l'entité locale? Quelles sont les restrictions spécifiques imposées par les différents pays?
- Le client veut-il protéger les assurés localement? Les polices locales offrent notamment les avantages suivants : indemnisation locale des pertes, libellé de police local et traitement local des réclamations.

### Capacités multinationales de Chubb en matière de cyberrisques :

**Chubb peut offrir des programmes d'assurance multinationaux contre les cyberrisques localement et couvre plus de 35 pays** dans le monde entier; les services sont offerts par les équipes de service mondiales de Chubb entièrement pourvues en personnel qui possèdent l'expertise et disposent des spécialistes nécessaires pour aider à répondre aux besoins en matière d'assurance multinationale.

## 2 Cyberinstallations mondiales

Une solution de gestion des cyberrisques élargie pour les grandes entreprises.

**À qui cette solution s'applique-t-elle?**

- Organisations dont le chiffre d'affaires annuel s'élève à plus de 1 G$.
- Tous les secteurs, y compris les commerces de détail, les institutions financières et les fabricants.

**Composantes de l'offre :**

- Services de contrôle préalables à l'événement offerts par des organisations de cyberdéfense réputées mondialement pour remédier aux lacunes en matière de cyberrisques relevées au cours de l'évaluation des risques.
- Politique de transfert des risques.
- Intervention en cas d'incident et gestion des réclamations postérieures à l'événement.

**Principales garanties :**

- **Montants de garantie de base de 30 M$ à 100 M$ du capital de Chubb** ayant un effet relutif sur le marché pour les grandes « tours » de couverture d'assurance.
- **Avenants « DIC/DIL » (différences de conditions/différences de limites) offerts pour combler les lacunes** entre les polices contre les cyberrisques, les risques divers et de biens.
- Formulaires de police flexibles offerts.

**Quel est le processus?**

- Début du processus de vente de manière proactive trois mois avant l'offre de marché.
- Évaluation exclusive de Chubb visant à analyser le profil de risque d'une organisation.
- Engagement direct entre le client et le service de souscription de Chubb.

# Grandes entreprises

## 3 Captives d'assurance

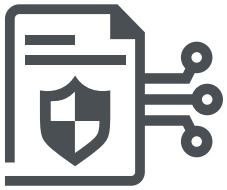
Gérer les cyberrisques dans une société d'assurance captive est devenu de plus en plus pertinent pour les sociétés multinationales pour lesquelles une combinaison de transfert des risques et de rétention du risque est utile. Les captives d'assurance sont une solution de plus en plus courante pour maintenir des primes adéquates, mais gérables, ou pour transférer des franchises de polices locales vers une structure consolidée.

Une captive peut également offrir à la société mère une couverture plus complète que celles offertes sur le marché de l'assurance des entreprises. Ainsi, l'entreprise est en mesure de comprendre ses expositions aux risques et de recueillir des informations sur les pertes afin qu'un assureur ou un réassureur puisse assumer le risque selon des limites et des primes adéquates.

| Pourquoi | Comment | Défis |
|---|---|---|
| • Optimisation du transfert des risques<br>• Diversification<br>• Rôle d'incubateur<br>• Accès à des services complémentaires | • Différentes structures possibles<br>• Niveaux de franchises faibles/élevés<br>• Quote-part de grands programmes<br>• Spécifique aux risques | • Incertitude/ compréhension de l'exposition<br>• Tarification des niveaux de rétention<br>• Agrégation avec d'autres catégories |

# Arguments de vente déterminants

**Vos clients ne comprendront pas tous l'importance d'une police d'assurance contre les cyberrisques ni tous les avantages qu'elle peut offrir. Nous avons réuni quelques arguments de vente déterminants pour vous aider à expliquer certains de ces avantages à vos clients.**



### Protection spécifique

Les polices d'assurance traditionnelles peuvent ne pas répondre adéquatement aux cyberrisques. Les polices d'assurance contre les cyberrisques sont précisément conçues pour corriger ces lacunes et vous offrir une protection spécifique contre des risques qui peuvent être difficiles à appréhender.

### Il n'est pas nécessaire que vous soyez la cible pour être touché

Les cyberattaques peuvent se propager à vos fournisseurs ou à vos fournisseurs de services technologiques impartis, ce qui peut avoir une incidence considérable même lorsque vous n'êtes pas la cible. Chubb a observé d'importants dommages collatéraux causés par des cyberincidents provenant de sociétés différentes. Que se passerait-il si votre fournisseur de services de stockage de données était la cible d'une cyberattaque compromettant la protection de vos données?

### L'assurance couvre les frais d'intervention et de récupération, et non seulement la responsabilité découlant de la compromission des données

La responsabilité découlant de la perte ou de l'utilisation abusive de données sensibles n'est que l'une des conséquences potentielles d'un cyberincident. Les coûts associés à l'interruption des activités, à l'intervention en cas d'incident et à la récupération des données numériques peuvent représenter une partie importante des indemnités versées par Chubb en cas de pertes, même en l'absence de réclamations en assurance responsabilité civile.

### Compléter les équipes de TI existantes

L'assurance contre les cyberrisques ne diminue pas l'efficacité des équipes de sécurité informatique – elle complète leurs compétences et protège l'entreprise contre l'inconnu.

# Arguments de vente déterminants

### Menaces multinationales

Les cyberpertes ne sont pas subies uniquement à l'échelle locale. Chubb aide les sociétés à se rétablir de cyberincidents survenant dans le monde entier, dont des atteintes à la protection des données, des attaques par rançongiciel et d'autres incidents.

### Toutes les entreprises peuvent être touchées

Les cyberincidents peuvent toucher n'importe quelle entreprise, quels que soient sa taille et son secteur d'activité. Les menaces peuvent être ciblées, des employés peuvent commettre des erreurs ou un cyberincident de plus grande envergure peut causer des dommages collatéraux. Chubb offre des solutions flexibles en fonction des besoins, du niveau de maturité et de la taille de l'entreprise.

### S'adapter à l'évolution de la réglementation

Les nouveaux règlements en matière de protection de la vie privée imposent des normes et des sanctions de plus en plus élevées – et l'assurance contre les cyberrisques peut vous aider à vous adapter à ces changements. Le libellé des polices de Chubb tient compte de la nouvelle réglementation en matière de protection de la vie privée et de son évolution.

### S'adapter aux cyberrisques émergents

Chubb communique les nouvelles tendances des réclamations en matière de cyberrisques sur une base trimestrielle, vous tenant ainsi au courant des nouveaux risques au fur et à mesure que nous en prenons connaissance. Le Chubb Cyber Index® vous donne également des informations à jour sur les tendances récentes et passées.

# Cyberservices

## Combler l'écart entre l'expertise en assurance contre les cyberrisques et l'expertise en cybersécurité.

Souscrire une assurance contre les cyberrisques auprès de Chubb est une excellente première étape qu'une organisation peut franchir pour contribuer à se protéger contre les pertes financières et de réputation qu'elle peut subir en cas d'atteinte à la protection des données et de panne de système. Mais la protection ne s'arrête pas là. Les titulaires de police de Chubb ont accès à un éventail d'outils d'atténuation essentiels et de ressources-conseils qui peuvent aider à réduire leur exposition en tout temps.

Aidez vos clients à utiliser la puissance de nos solutions et de nos ressources-conseils dès aujourd'hui. Pour demander des informations sur les services ou pour planifier une rencontre d'orientation avec un conseiller en cyberrisques de Chubb, veuillez visiter le site à l'adresse www.chubb.com/ca-fr/business-insurance/getcyberservices.html ou nous envoyer un courriel à cyber@chubb.com.

**Pour vous inscrire** aux services et pour obtenir de plus amples renseignements, veuillez visiter le site Web des cyberservices de Chubb :

**www.chubb.com/ca-fr/getcyberservices**

# Cyberservices

## Solutions d'intervention en cas de cyberincident

Déployer des outils et des évaluations qui peuvent aider à détecter des risques de cybersécurité et à y faire face avant qu'un incident ne survienne.

Application mobile pour les interventions en cas d'incident | Générateur en ligne de plans d'intervention cybernétique | Exercice de simulation virtuel pour les plans d'intervention en cas de cyberincident | Évaluation de la rapidité d'intervention

## Solutions de gestion de la cybervulnérabilité

Surveiller de près les vulnérabilités des logiciels et des réseaux qui pourraient avoir une incidence sur les résultats.

Système d'alerte de Chubb sur les cybervulnérabilités | Service de surveillance des vulnérabilités externes | Analyse de la vulnérabilité des réseaux

## Solutions de cybersécurité des points d'extrémité

Obtenir des solutions qui vous aideront à empêcher des attaques malveillantes de pénétrer et se propager dans un réseau.

Solution de sécurité des points d'extrémité et d'intervention en cas d'incident | Gestion des correctifs

## Solutions de sécurité et d'éducation des utilisateurs

Créer et maintenir un effectif qui agira comme première ligne de défense.

Solutions d'évaluation et de mise en œuvre de l'authentification multifactorielle | Gestionnaire de mots de passe sécurisé | Simulateur de courriels d'hameçonnage | Sécurité périphérique des courriels | Formation sur la sensibilisation à la sécurité | Bibliothèque de ressources en cyberrisques


**Apprenez-en davantage**

Communiquez avec notre Équipe de conseillers en cyberrisque

Visitez le site à l'adresse chubb.com/ca-fr/getcyberservices

# Couverture – Gestion des cyberrisques d'entreprise

## Couverture

### Risques propres

- **Intervention en cas d'incident** – à la suite d'un cyberincident avéré ou suspecté
- **Interruption des activités de l'entreprise** – perte de bénéfice net et frais d'exploitation toujours engagés
- **Récupération des données numériques** – augmentation du coût des travaux, de récupération des données et d'atténuation de l'interruption des activités
- **Extorsion visant un réseau** – paiements et négociation en cas d'extorsion

### Tiers

- **Responsabilité en matière de cybercriminalité, de respect de la vie privée et de sécurité des réseaux** – responsabilité à la suite d'une atteinte à la protection des données ou d'une défaillance de sécurité de réseau :
  - **Perte de carte de paiement** et responsabilités contractuelles envers des sociétés du secteur des cartes de paiement par suite d'un cyberincident
  - **Fonds de recours des consommateurs**
  - **Amendes réglementaires** et sanctions (lorsque la loi permet d'assurer ces risques)
- **Responsabilité des médias** – responsabilité à la suite de diffamation ou de violation en ligne

## Principaux éléments

- **Pertes d'exploitation éventuelles** pour les tiers fournisseurs de services technologiques impartis
- **Défaillance de réseau** – comprend erreurs humaines, erreurs de programmation ou pannes de courant
- **Extensions standards :**
  - **Dépenses d'intervention d'urgence en cas d'incident** dans un délai de 48 heures pour les PME et les clients du marché intermédiaire assurés
  - **Coûts d'amélioration** - amélioration de logiciel et d'applications
  - **Cybercriminalité** – perte financière directe après un cybervol
  - **Dépenses liées aux récompenses**
  - **Fraude de télécommunications**
- **Paiement au nom de l'assuré** des frais d'intervention en cas d'incident
- **Employé sans scrupules**
- **Avis volontaire**
- **Fermeture volontaire***
- **Atteinte à la réputation***
- **Fraude par piratage psychologique***
- **Territoire de la couverture universelle** – s'applique aux incidents et aux réclamations
- Première introduction d'une couverture des cyberévénements généralisés de l'industrie

* Par avenant

# Avenants

**Chubb a adopté une approche flexible et durable face à l'augmentation des cyberrisques. Les titulaires de police peuvent personnaliser les niveaux de couverture d'assurance contre les cyberrisques pour les événements généralisés, les attaques par rançongiciels et les vulnérabilités logicielles négligées.**

## 1 Événements généralisés

Le monde devient de plus en plus numérique et interconnecté d'année en année. Des milliers d'entreprises, voire des millions, utilisent des programmes logiciels, des plateformes de communication et des plateformes technologiques et souvent, elles en dépendent. Une seule attaque ciblant une de ces plateformes ou technologies largement utilisées ou la défaillance de celles-ci pourrait entraîner un risque d'agrégation qui excède la capacité de l'industrie de l'assurance à les garantir. Afin d'offrir aux titulaires de police des garanties claires et une stabilité par rapport au marché, Chubb offre des limites, des montants de rétention spécifiques et une coassurance pour de tels événements généralisés.

**Voici certains types de risques d'événements généralisés couverts :**

- **Attaques généralisées sur une chaîne d'approvisionnement logicielle**
  Ces attaques permettent à des individus malveillants d'accéder à des systèmes au moyen de logiciels de confiance certifiés et d'introduire un cheval de Troie dans un système.
- **Exploitations généralisées d'une vulnérabilité du jour zéro**
  Ces attaques découlent de certaines vulnérabilités logicielles qui sont connues seulement des cybercriminels – des vulnérabilités pouvant être facilement exploitées, qui sont graves et manquent souvent de protection.
- **Exploitation généralisée d'une vulnérabilité sévère connue**
  Ces attaques découlent de vulnérabilités logicielles graves connues qui ne sont pas corrigées. Les vulnérabilités sont considérées comme graves parce qu'elles sont faciles à exploiter, peuvent être déployées à distance avec des privilèges d'accès limités, et peuvent avoir une incidence négative importante[1].
- **Tous les autres événements généralisés**
  Certains types de cyberattaques peuvent être menées simultanément ou automatiquement contre un nombre élevé de victimes, causant au bout du compte un cyberévénement catastrophique. Internet et certains services de télécommunications se sont élevés au rang d'infrastructures sociétales d'importance critique, et l'utilisation de certaines grandes entreprises d'informatique en nuage est si répandue qu'une panne pourrait avoir des conséquences sur les activités de milliers d'entreprises, voire de millions.

**Exemples concrets de risques d'événements généralisés :**

- Attaque généralisée sur une chaîne d'approvisionnement logicielle : Solorigate (2020), NotPetya (2017)
- Exploitation généralisée d'une vulnérabilité du jour zéro : Hafnium (2021)
- Exploitation généralisée d'une vulnérabilité sévère connue : attaque envers un fournisseur de services de sécurité gérés (MSSP) (2021)
- Autre événement généralisé : panne de nuage informatique en Virginie (2020)

**L'avenant pour événements généralisés de Chubb énonce des règles concises et sensées de règlement de sinistres, dont les suivantes :**

- Les frais d'intervention en cas d'incident ne diminueront pas les limites de garantie pour les événements généralisés tant qu'il n'a pas été établi qu'un incident est un événement généralisé, et les dépenses engagées avant ce moment n'auront pas à être remboursées.
- Les titulaires de police peuvent décider de ne pas partager certains types de données d'enquête lorsqu'il est mutuellement convenu qu'un incident est un événement généralisé.
- Tous les cyberincidents entrent soit dans la catégorie des événements avec incidence limitée (p. ex., un événement local avec des mesures de règlement des sinistres qui prescrivent de mener les activités comme d'habitude) ou des événements généralisés (p. ex., un événement systématique avec des écarts de règlement des sinistres structurels touchant notamment la limite, la rétention et la coassurance), ce qui permet aux titulaires de police de souscrire la garantie qui répond le mieux aux besoins de leur entreprise.

[1] *NIST Security Vulnerability Trends in 2020: An Analysis* (2021). https://www.redscan.com/media/Redscan_NIST-Vulnerability-Analysis-2020_v1.0.pdf.

# Avenants

## 2 Rançongiciels

La fréquence et la gravité des attaques par rançongiciel ont augmenté de façon spectaculaire. Les pertes que cela implique pour les titulaires de police vont bien au-delà de la seule valeur du montant de la rançon. Qu'ils paient ou non la rançon, les titulaires de police engagent souvent des frais juridiques, des frais d'enquête judiciaire, des pertes d'exploitation, des coûts de récupération des données numériques, et, potentiellement, des coûts de responsabilité et des frais de défense juridique.

L'avenant relatif aux incidents de rançongiciel permet de personnaliser les limites de garantie, la rétention et la coassurance pour les pertes subies par suite d'un incident de rançongiciel.

## 3 Vulnérabilités logicielles négligées

Tenir les logiciels à jour est un aspect important d'une bonne hygiène en matière de cyberrisques. De nombreuses pertes peuvent être prévenues en corrigeant les logiciels vulnérables avant que des cybercriminels n'aient la chance de les exploiter, mais certaines organisations peuvent ne pas corriger les logiciels immédiatement. Il y a parfois des raisons légitimes pour lesquelles des mises à jour logicielles doivent être testées avant leur déploiement, et des problèmes de compatibilité, de capacité ou simplement de logistique peuvent empêcher une organisation spécialisée en sécurité de déployer des correctifs dès le premier jour ou la première semaine où ils sont rendus disponibles. Pour cette raison, Chubb offre à ses titulaires de police un délai de grâce de 45 jours pour corriger des vulnérabilités logicielles qui sont inscrites comme faille et vulnérabilité commune (Common Vulnerabilities and Exposures, CVE) dans la National Vulnerability Database exploitée par le National Institute for Standards and Technology (NIST) des États-Unis.

L'avenant relatif aux vulnérabilités logicielles négligées procure une garantie après la fin du délai de grâce de 45 jours, le partage des risques entre le titulaire de police et l'assureur passant graduellement au titulaire de police, qui assume progressivement de plus en plus de risque si la vulnérabilité n'est pas corrigée après 45, 90, 180 et 365 jours.

# Appétit de souscription

Pour vous aider à mieux servir vos clients, nous avons créé le résumé suivant de notre appétit de souscription. Cette liste n'est pas exhaustive, mais elle donne des lignes directrices générales. Veuillez communiquer avec notre équipe de souscription pour discuter de vos besoins relativement à des risques ou des secteurs qui ne sont pas énumérés ci-dessous.

## Privilégié

- Agriculture
- Architectes et ingénieurs
- Associations sans but lucratif
- Communications*
- Concessionnaires automobiles et stations-service
- Construction
- Consultants en gestion
- Consultants en marketing
- Consultants techniques
- Entrepreneurs généraux
- Exploitation minière
- Fabrication de produits
- Fabrication industrielle
- Galeries d'art et musées
- Grossistes
- Immobilier
- Imprimerie et édition*
- Ingénierie et gestion/Services
- Production alimentaire/ Fabrication
- Production télévision/ radio/cinéma*
- Produits chimiques et produits connexes
- Publicité*

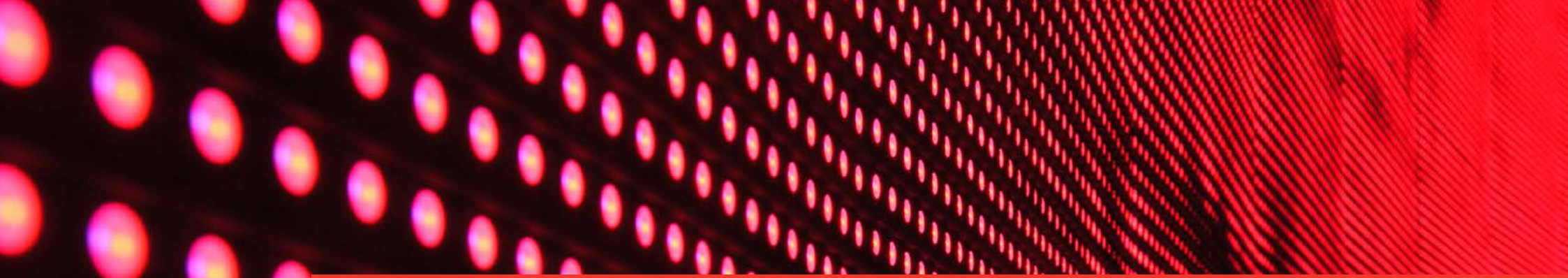
## Accepté

- Agence de placement/ Agence de recrutement
- Arts du spectacle et théâtres*
- Associations professionnelles
- Cabinets d'avocats – sociétés
- Cabinets de médecins et de dentistes
- Comptables
- Courtiers hypothécaires
- Gestionnaires d'actifs
- Gestionnaires de placements/ de fonds
- Institutions de dépôt
- Institutions financières – non énumérées
- Intervenants en matière de santé connexes
- Matériel et logiciels
- Restauration/Hôtellerie
- Services de transport – non énumérés
- Services personnels
- Services professionnels – non énumérés
- Vente au détail

## Sélectif

- Administration publique
- Agences de recouvrement
- Agents de titres
- Assurance – autres que des particuliers
- Autorité publique/ District spécial
- Banque d'épargne de détail
- Bureaux de change
- Centres d'appel
- Collèges et universités
- Courtiers en valeurs mobilières et produits de base
- Gouvernement
- Hôpitaux
- Maison de soins infirmiers/ Résidence pour personnes âgées
- Négociateurs de marchandises
- Notaires
- Petites écoles/Conseils scolaires de la prématernelle à la 12e année
- Radiodiffusion*
- Résidences-services
- Services de facturation
- Services de télémarketing*
- Services publics
- Télécommunications

* Non inclus dans les assurances erreurs et omissions pour les médias



CHUBB®

# Renseignements supplémentaires

Pour en apprendre davantage sur notre offre en assurance contre les cyberrisques, veuillez communiquer avec nos souscripteurs ou visiter le site **www.chubb.com/cyber**.

Retour au début