

# Gestion des cyberrisques d'entreprise

Une approche durable pour contrer une vaste gamme d'incidents cybernétiques, y compris les événements généralisés

CHUBB®



Cela fait plus de 20 ans que Chubb gère des cyberincidents et souscrit des cyberrisques pour les titulaires de ses polices.

Au fil du temps, le monde s'est transformé en un réseau de technologies et de données de plus en plus interconnecté. Aujourd'hui, les entreprises sont confrontées à de nombreux risques cybernétiques. Plusieurs d'entre eux sont des risques systémiques partagés qui peuvent toucher un éventail d'entreprises. Ces risques systémiques peuvent causer des événements généralisés et entraîner des pertes catastrophiques. Des solutions à l'échelle de l'entreprise sont nécessaires pour adresser ces risques affectant toute l'entreprise : Gestion des cyberrisques d'entreprise (GCE) de Chubb.

Grâce à l'approche GCE de Chubb en matière de couverture des événements généralisés, les entreprises peuvent adapter la couverture d'assurance à leurs risques et à leurs besoins uniques, ce qui offre une plus grande certitude en matière de couverture et assure également une stabilité à long terme sur le marché de la cyberassurance.

## GCE offre une approche à trois volets :

---

- Services d'atténuation des pertes - accès aux outils et ressources nécessaires pour traiter et évaluer les principaux risques de cybersécurité avant qu'un événement ne se produise.
- Services d'intervention en cas d'incident - une équipe diversifiée d'experts en droit, informatique, notifications, centres d'appels, relations publiques, services de consultation en matière de fraude, de surveillance du crédit et de restauration de l'identité qui ont pour objectif d'aider à limiter les expositions aux risques de pertes lorsqu'un événement se produit.
- Transfert de risque - couverture étendue et durable soutenue par la solidité financière du bilan de Chubb.

## Avantages concurrentiels

---

- Principal fournisseur de solutions pour cyberrisques depuis le lancement de notre premier produit en 1998.
- Des solutions innovantes et hautement personnalisables pour répondre aux besoins uniques des clients, quels que soient leur taille, leur secteur d'activité ou leur type de risque.

- Aucune prime minimum. Échelle de prime pour les risques de toute taille, basée sur l'étendue de la couverture et les limites.
- Couverture pour cybercrimes offerte sous forme d'avenant ou d'assurance indépendante, dans la gamme d'assurances détournements ou vols et détournements de Chubb.
- Couverture des frais engagés pour gérer un cyberincident avec solutions étendues, axées sur le client et allant au-delà des exigences réglementaires.
- Création de devis en ligne et émission de police en temps réel pour les risques faibles admissibles. Les risques référés seront traités rapidement par votre souscripteur Chubb.
- Couverture d'assurance novatrice conçue pour répondre à l'évolution des normes réglementaires, juridiques et de cybersécurité et mise au point pour tenir compte de changements futurs.

- Produit d'assurance facile à lire conçu en fonction du déroulement d'un cyberincident typique, ce qui facilite la prise de décision tout au long du processus.
- Étendue territoriale des garanties applicable dans le monde entier pour adresser l'évolution constante des services d'hébergement et de stockage des données.

#### **Nouveaux avenants introduits en 2021**

- L'avenant pour événements généralisés vise à résoudre les incidents ayant un impact étendu et touchant les parties sans lien avec l'assuré. Tout comme les risques d'inondation et de tremblement de terre sont prévus dans les polices d'assurance des biens, la couverture, les limites, les rétentions et la coassurance peuvent être adaptées pour tous les événements généralisés ou pour des risques spécifiques :

- Exploitation généralisée d'une vulnérabilité sévère
- Exploitations généralisées d'une vulnérabilité du jour zéro
- Attaques généralisées sur une chaîne d'approvisionnement logicielle
- Autres événements systémiques
- L'avenant Rançongiciel vise à contrer le risque croissant des rançongiciels en proposant un ensemble adapté de limites de couverture, de montants de rétention et de coassurance qui s'appliquent uniformément à toutes les couvertures cybernétiques.
- L'avenant relatif aux vulnérabilités logicielles négligées reconnaît et récompense les bonnes pratiques en matière d'hygiène des correctifs logiciels en fournissant une couverture complète pendant 45 jours, puis en rééquilibrant progressivement le partage des risques entre l'assuré et l'assureur pour les logiciels qui ne sont pas corrigés au-delà de 45 jours.

#### **Aperçu des couvertures**

Les couvertures suivantes sont offertes dans le cadre de l'assurance GCE :

##### **Couverture de la responsabilité civile des tiers**

- **Responsabilité civile en matière de cyberrisques, de renseignements confidentiels et de sécurité du réseau :** Omission de protéger les renseignements personnels d'autres personnes et omission d'empêcher un cyberincident d'affecter les systèmes de tiers.
- **Perte liée à une carte de paiement :** Responsabilités contractuelles envers des sociétés du secteur des cartes de paiement par suite d'un cyberincident
- **Procédure réglementaire :** Défense contre les actions réglementaires et couverture des amendes et pénalités, si elles sont assurables en vertu de la loi.
- **Responsabilité des médias :** Violation des droits d'auteur et des marques de commerce liés à un contenu médiatique défini.

##### **Couverture des risques propres :**

- **Fonds d'intervention en cas de cyberincident :** Honoraires juridiques, enquêtes informatiques, frais de notification, surveillance des créances, relations publiques, etc.
- **Perte d'exploitation :** Perte de bénéfices et dépenses résultant de l'interruption des systèmes de l'assuré et autres frais supplémentaires; la garantie Pertes d'exploitation éventuelles couvre également les pertes résultant de l'interruption des systèmes de tiers.
- **Recouvrement des données numériques :** Frais engagés pour restaurer ou remplacer les données et les logiciels perdus ou endommagés.
- **Fraude téléphonique :** Dépenses encourues sous forme de frais téléphoniques à la suite d'appels frauduleux.
- **Extorsion visant un réseau :** Paiement pour prévenir la destruction ou l'endommagement des données numériques.

##### **Cybercriminalité (sous réserve d'un avenant)**

- **Fraude informatique :** Accès par un tiers aux ordinateurs de l'assuré en vue de dérober des fonds.
- **Fraude liée aux virements de fonds :** Fraude commise par un tiers sur une banque pour transférer des fonds du compte d'un assuré.
- **Fraude par ingénierie sociale :** Usage de moyens frauduleux par un tiers pour inciter un employé à transférer de l'argent.

#### **Nous contacter**

Pour en savoir plus sur la GCE, communiquez avec votre souscripteur local ou visitez le [www.chubb.com/ca-fr](http://www.chubb.com/ca-fr).

**Chubb. Insured.<sup>SM</sup>**