# Guide sur les réclamations en matière de cybersécurité

**RENSEIGNEMENTS ESSENTIELS DE L'ÉQUIPE MONDIALE DES CYBERRISQUES DE CHUBB**

CHUBB®

# Table des matières

Depuis 25 ans, Chubb offre des solutions de cyberassurance robustes, renforcées par une richesse de données historiques sur les sinistres et un sens aigu de la souscription, tous orientés vers une sélection optimale des risques.

Dans la première édition du Rapport sur les réclamations en matière de cybersécurité de Chubb, nous explorons les données historiques sur les réclamations de Chubb jusqu'en décembre 2024. Ainsi, nous dévoilons des renseignements sur les tendances en matière de fréquence et de gravité, les incidents liés aux rançongiciels et les réclamations en matière de protection des renseignements personnels afin d'aider les entreprises à composer avec les complexités de l'environnement de cyberrisques d'aujourd'hui.

**1999** Chubb commence à offrir des solutions d'assurance contre les cyberrisques.

**2014** Chubb lance sa gamme de **Services d'atténuation des pertes** la première dans son genre.

**2018** Chubb présente le premier indice de réclamations du marché, l'outil **Cyber Index de Chubb**, accompagné de nos bulletins d'information trimestriels **Cyber InFocus**.

**2025** Chubb lance la première édition du Rapport sur les réclamations en matière de cybersécurité de Chubb.

*Les données relatives aux sinistres et aux pertes contenues dans ce rapport sont exclusives et basées uniquement sur les réclamations de Chubb, sauf indication contraire*

Au cours des 24 derniers mois, la fréquence et la gravité des réclamations en matière de cybersécurité ont augmenté, même si les entreprises que nous assurons sont devenues plus sûres.

Les réclamations sont devenues plus graves en raison des incidents liés aux rançongiciels, mais plusieurs événements généralisés ont contribué à l'augmentation de leur fréquence en 2024. De plus, la responsabilité en matière de protection des renseignements personnels est devenue une source plus importante de réclamations, notamment en raison de décisions judiciaires récentes et de nouvelles théories juridiques de la responsabilité qui ont été avancées. Ces tendances ont eu une incidence sur des clients de tailles, de régions et de secteurs différents selon des mesures variables.

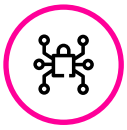
L'expérience de Chubb en matière d'assurance contre les cyberrisques depuis plus de vingt ans a permis de tirer des conclusions qui sont confirmées par nos propres données internes sur les sinistres cybernétiques. Ces conclusions

## Voici quelques principaux points à retenir :

La fréquence et la gravité des réclamations en matière de cybersécurité continuent de croître aux États-Unis, surtout pour les clients de grande envergure dont les revenus dépassent 1 milliard de dollars. À l'extérieur des États-Unis, toutefois, la fréquence et la gravité des réclamations diminuent.

Les incidents liés aux rançongiciels demeurent le principal moteur des réclamations d'assurance Cyber et de la gravité des pertes. Les auteurs de menaces devenant de plus en plus sophistiqués, les entreprises de toutes tailles doivent être prêtes à déterminer si elles paieraient une rançon et à supporter les conséquences opérationnelles de cette décision.

La responsabilité en matière de protection des renseignements personnels devient plus complexe à mesure que les législateurs du monde entier adoptent ou modifient des lois régissant la collecte, la communication et l'utilisation de données biométriques et d'autres renseignements personnels. Les entreprises et les organisations doivent se tenir au courant de l'incidence de ces règlements et s'assurer de respecter les règlements en fonction de leurs activités.

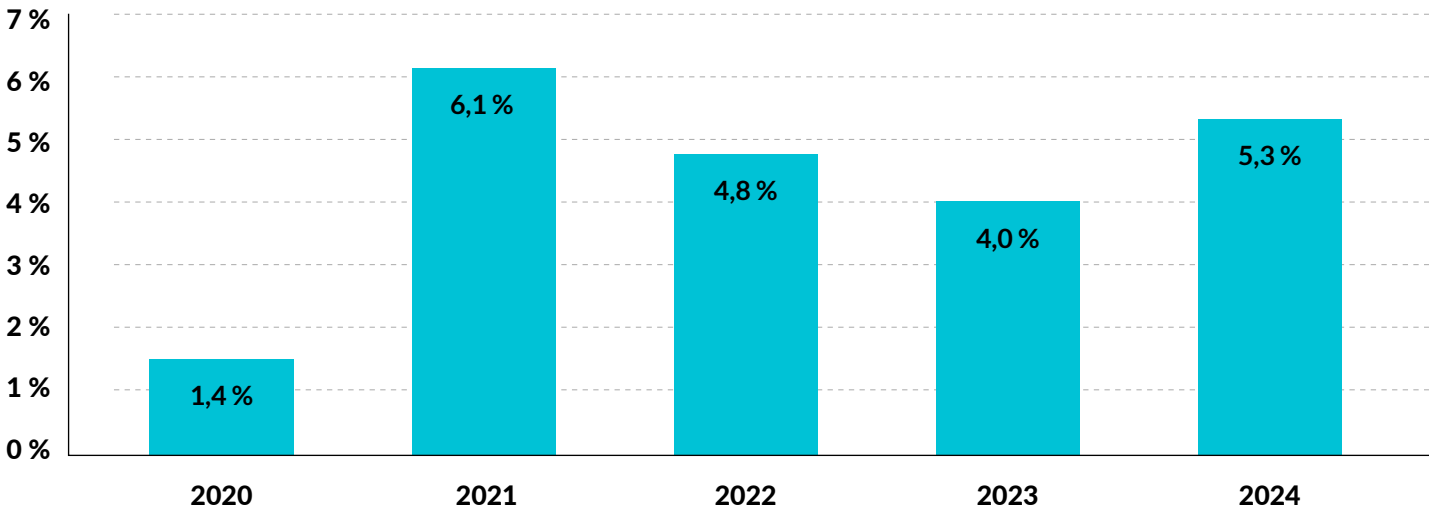


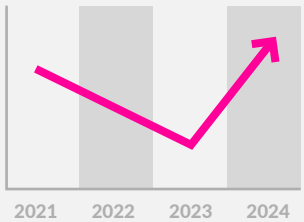
L'une des meilleures façons pour les organisations de s'armer contre un cyberincident débilitant est d'adopter une stratégie qui combine un modèle de sécurité à vérification systématique et une sensibilisation accrue des dirigeants et des employés aux risques.

# Fréquence et gravité des cyberincidents

Peu d'assureurs disposent d'une envergure mondiale et d'une diversité d'activités couvrant toutes les tailles de clients et tous les secteurs, qui leur permettraient d'identifier des tendances crédibles et détaillées en matière de réclamations. Les contrôles de sécurité et la résilience des clients ont contribué à atténuer l'incidence des cybermenaces. Cependant, les événements cybernétiques généralisés, qui peuvent être enracinés dans des attaques, ainsi que les défaillances logicielles ou les erreurs humaines, causent des perturbations économiques et opérationnelles importantes et deviennent plus fréquents.

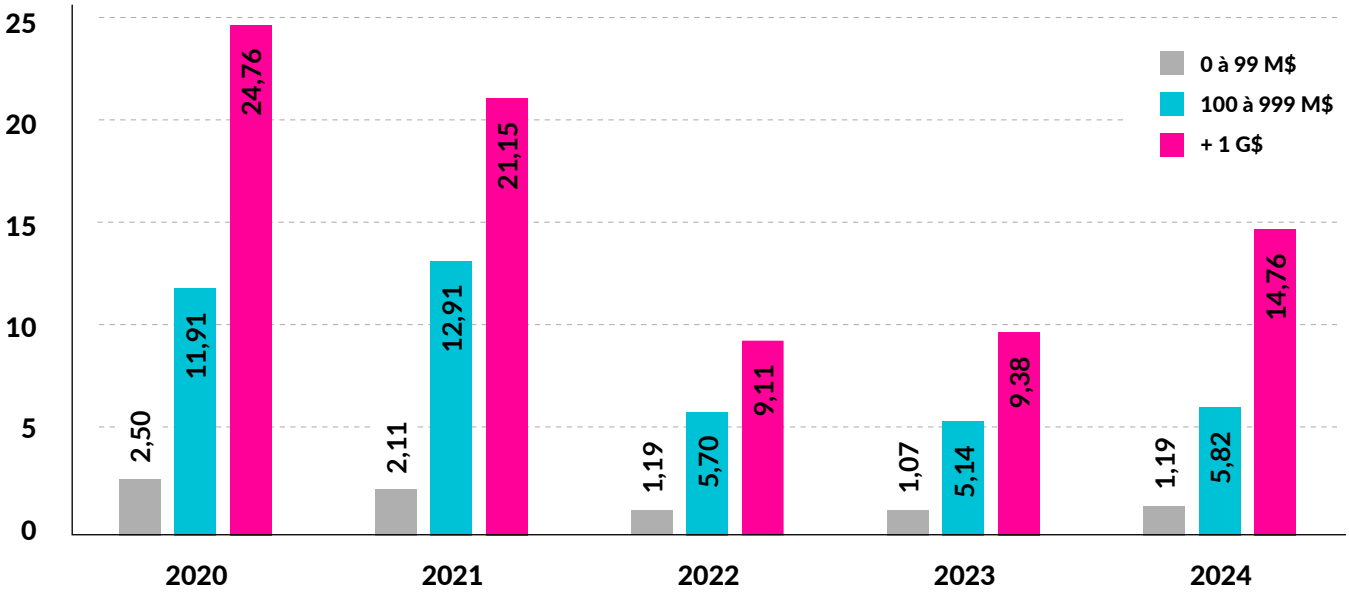
## Pourcentage du nombre total de réclamations en matière de cybersécurité déclarées découlant d'événements systémiques au cours de l'année civile




Nos données sur les réclamations en témoignent : Bien qu'il ait diminué de 2021 à 2023, le pourcentage du nombre total de réclamations en matière de cybersécurité déclarées découlant d'événements systémiques — constituant des événements uniques qui touchent de nombreuses entreprises en même temps — a encore augmenté en 2024 et continue d'avoir une incidence sur la fréquence globale.

Fréquence des réclamations en matière de cybersécurité pour 100 polices d'assurance Cyber émises par tranche de revenus des assurés (États-Unis)



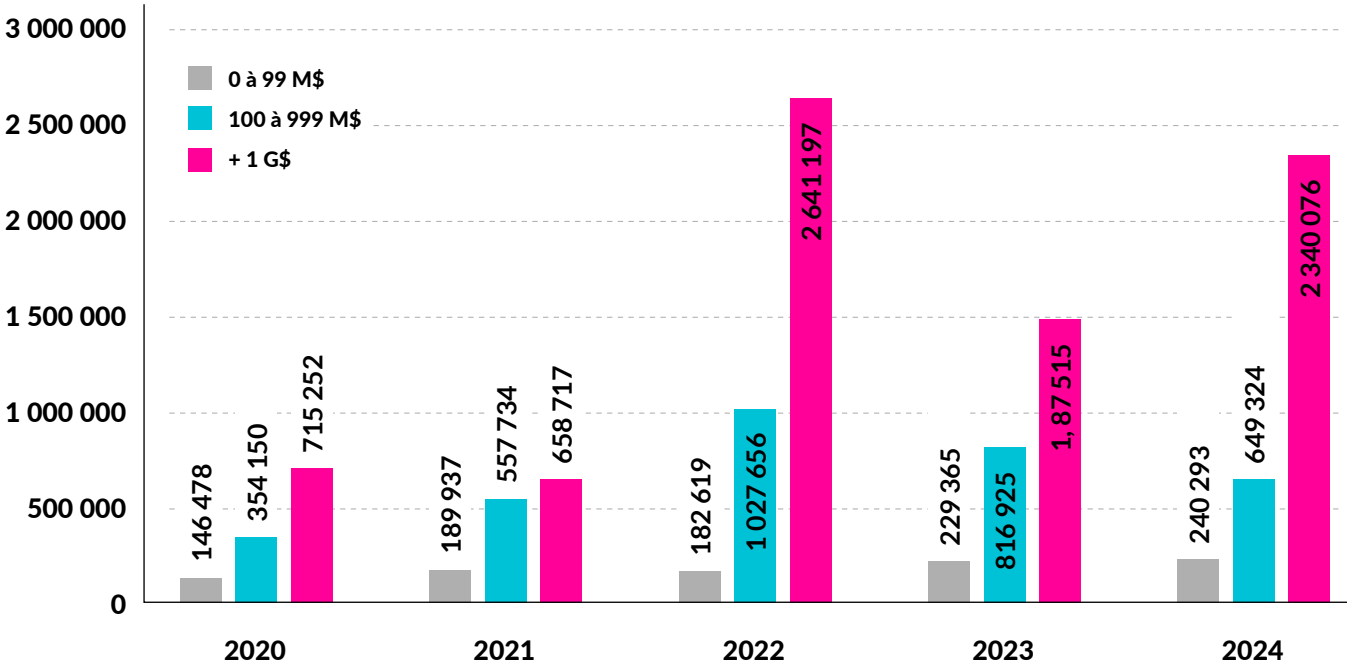

# 275 %

**Augmentation des attaques par rançongiciel au niveau mondial**

Microsoft a observé une augmentation de 275 % d'une année sur l'autre des attaques par rançongiciel opérées par des humains entre juillet 2023 et juin 2024. Cette augmentation des attaques par rançongiciel a été partiellement compensée par une diminution soutenue

Source: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf

## Gravité des réclamations en matière de cybersécurité par tranche de revenus des assurés (États-Unis)




La fréquence des réclamations en matière de cybersécurité pour les clients de Chubb aux États-Unis a augmenté au cours des trois dernières années, mais reste inférieure au sommet de 2020-2021, tandis que la gravité de ces réclamations a augmenté de 2020 à 2024, avec une volatilité importante au cours des trois dernières années. Les comptes de revenus moyens et élevés ont connu une forte augmentation de la gravité de 2022 à 2024, plusieurs grandes entreprises ayant présenté des réclamations importantes qui ont été largement publicisées dans les médias. Bien que les rançongiciels aient été en fin de compte un facteur important de l'augmentation de cette gravité, on doit noter que les acteurs malveillants ont commencé à utiliser de nouvelles tactiques. Certaines des attaques les plus remarquables n'ont pas été causées par des logiciels malveillants sophistiqués qui ont réussi à échapper aux mesures de cybersécurité de ces entreprises hautement contrôlées, mais plutôt par des **attaques de piratage psychologique**[1] comportant la manipulation des **centres de soutien technique des assurés**[2] et la **fraude par usurpation de carte SIM**.[3]

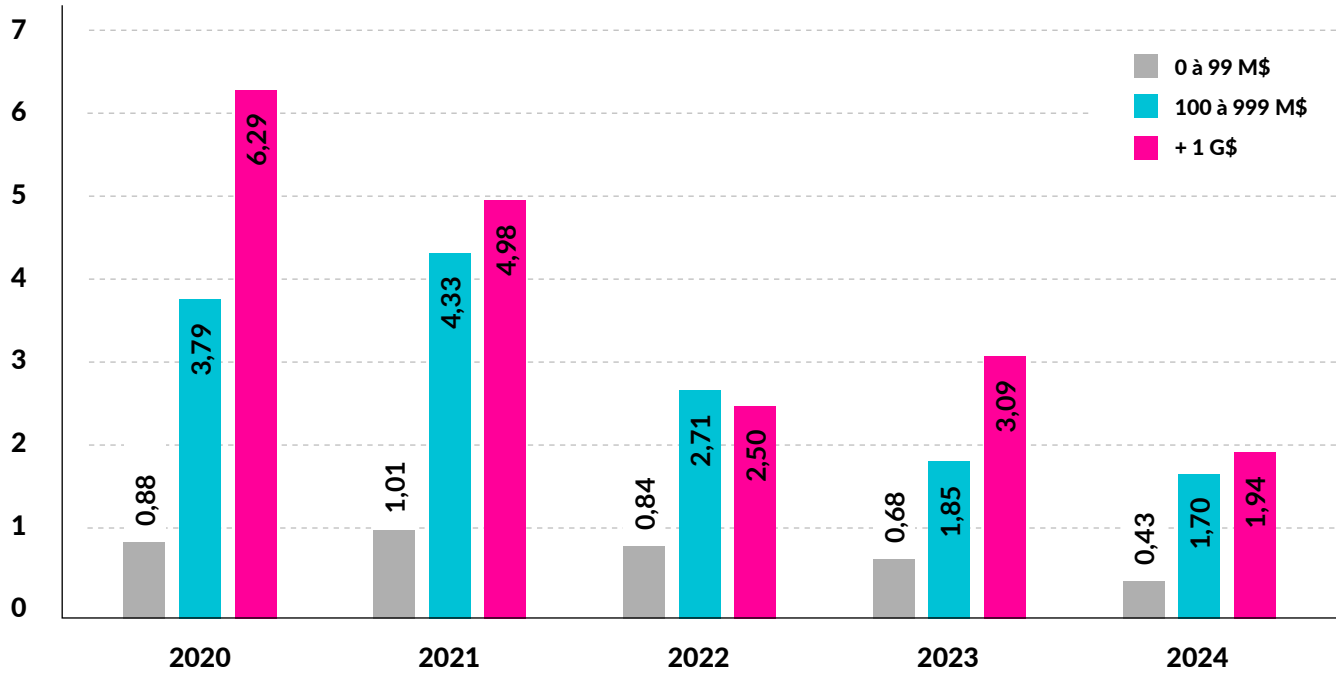
À l'heure actuelle, une plus grande part des réclamations subséquentes en matière de responsabilité de tiers aux États-Unis – pour les risques de toutes tailles – provient d'incidents liés aux rançongiciels et de litiges liés à la protection des renseignements personnels par rapport aux années précédentes.

1. Source: https://www.ibm.com/think/topics/social-engineering#:~:text=Social%20engineering%20attacks%20manipulate%20people,their%20personal%20or%20organizational%20security.
2. Source: https://www.obsidiansecurity.com/blog/understanding-social-engineering-attacks-on-helpdesk-agents/#:~:text=This%20technique%20typically%20begins%20with,to%20ensure%20their%20own%20persistence.
3. Source: https://www.incognia.com/the-authentication-reference/what-is-sim-swap-attack-and-why-fast-detection-is-important#:~:text=A%20SIM%20swap%20attack%20combines,to%20the%20fraudster's%20SIM%20Card.

## En revanche, la fréquence et la gravité des réclamations ont diminué dans les sociétés de toutes tailles à l'extérieur des États-Unis.

À l'instar de leurs homologues américains, les clients de Chubb à l'extérieur des États-Unis ont investi dans la cybersécurité en sensibilisant davantage la haute direction et le conseil d'administration aux cyberrisques, en renforçant la résilience par l'amélioration de la **planification de la continuité des activités**[1] et **l'utilisation de plans d'intervention en cas d'incident**,[2] et en se concentrant sur la conformité aux nouvelles structures réglementaires (comme la réglementation **Digital Operational Resilience Act** de l'UE)[3]. De plus, nous avons constaté une augmentation du nombre de clients qui ne veulent pas payer de rançons Cette combinaison de facteurs, conjuguée au fait que bon nombre de ces pays sont caractérisés par des cultures d'affaires moins litigieuses, a entraîné ces tendances favorables pour les clients à l'extérieur des États-Unis.

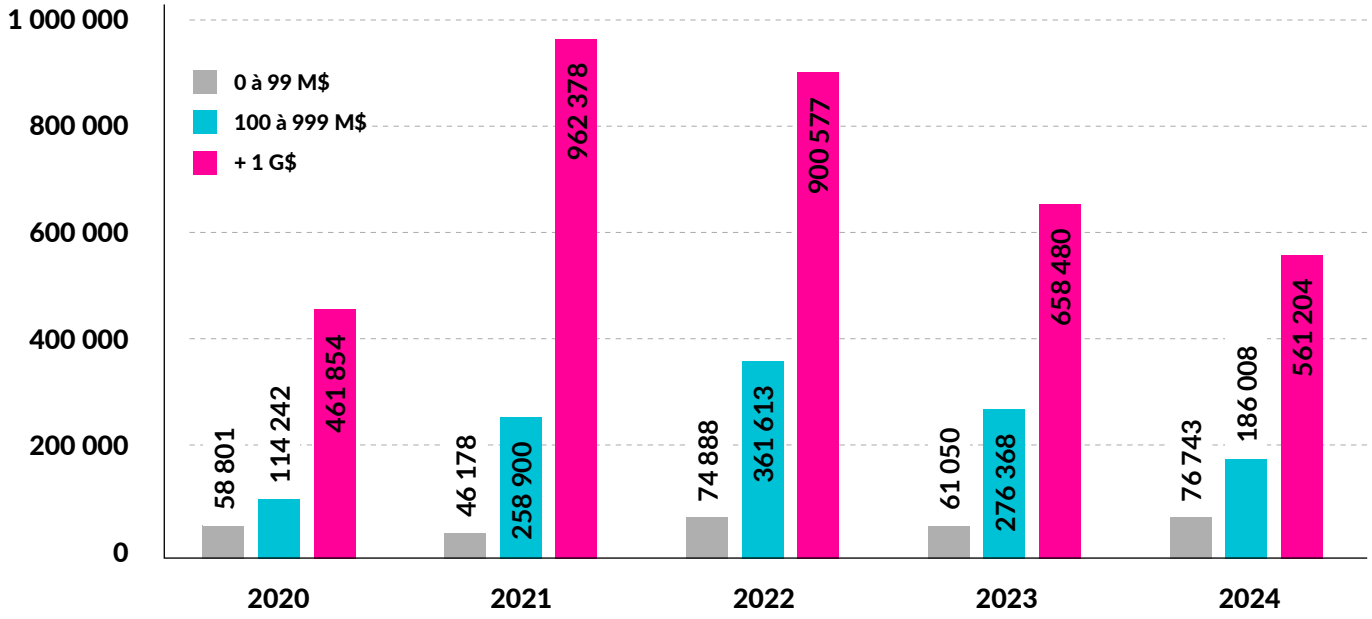
## Fréquence des réclamations en matière de cybersécurité pour 100 polices d'assurance Cyber émises par tranche de revenus des assurés (hors des États-Unis)




La fréquence a diminué pour les assurés de toutes tailles.

1. Source: https://www.institutedata.com/us/blog/business-continuity-planning-in-cybersecurity/
2. Source: https://www.ibm.com/think/topics/incident-response
3. Source: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

## Gravité des réclamations en matière de cybersécurité par tranche de revenus des assurés (hors des États-Unis)



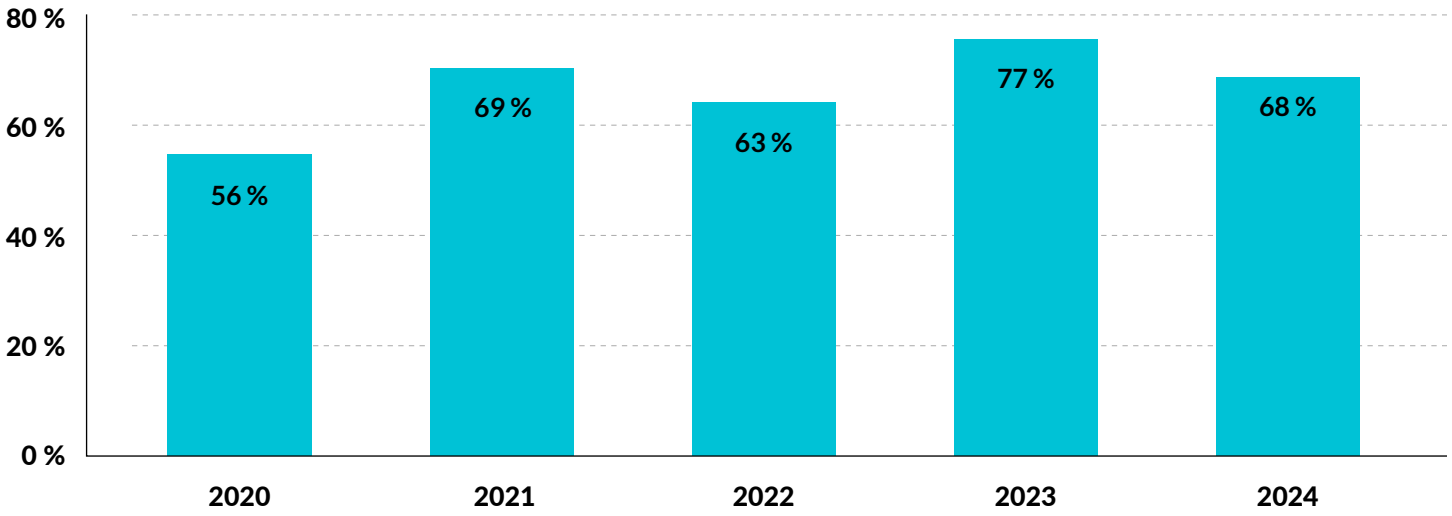

La gravité a diminué au cours des trois dernières années pour les moyennes et grandes entreprises, tandis que les petites entreprises ont connu une légère augmentation de la gravité au cours des dernières années.

# Le dilemme des rançongiciels - Payer ou ne pas payer?

Les événements de type rançongiciel sont à l'origine de la plupart des pertes liées aux cyberincidents à l'échelle mondiale, mais les clients réagissent différemment à un événement selon la solidité de leur plan de résilience. En raison de la complexité inhérente et du caractère urgent des réclamations relatives aux rançongiciels, les entreprises touchées sont confrontées à la difficile décision de payer ou de ne pas payer une rançon. Les auteurs de menaces reconnaissent que ces entreprises font face à un certain nombre de problèmes financiers, éthiques et juridiques. Ces acteurs pourraient bien utiliser cet environnement stressant à leur avantage, en doublant leurs efforts d'extorsion (en exigeant une rançon à la fois pour rétablir les systèmes et empêcher la divulgation) ou même en les triplant (en exigeant une rançon supplémentaire pour éviter une menace aux opérations ou à un tiers). Une entreprise qui paie une rançon peut prévenir d'autres dommages, mais les coûts associés à la reconstruction de ses systèmes, à la récupération des données et à l'avis aux clients peuvent tout de même être importants. Le non-paiement d'une rançon, en revanche, pourrait exposer une société à des pertes d'exploitation accrues ou à une responsabilité juridique supplémentaire. Dans le but de mettre un terme aux activités des rançongiciels, la Cybersecurity & Infrastructure Security Agency (Agence de cybersécurité et de sécurité des infrastructures) des États-Unis a mis sur pied un groupe de travail conjoint sur les rançongiciels. Celui-ci a publié un guide informatif intitulé à juste titre le **Guide #StopRansomware**.

Source: https://www.cisa.gov/stopransomware/ransomware-guide

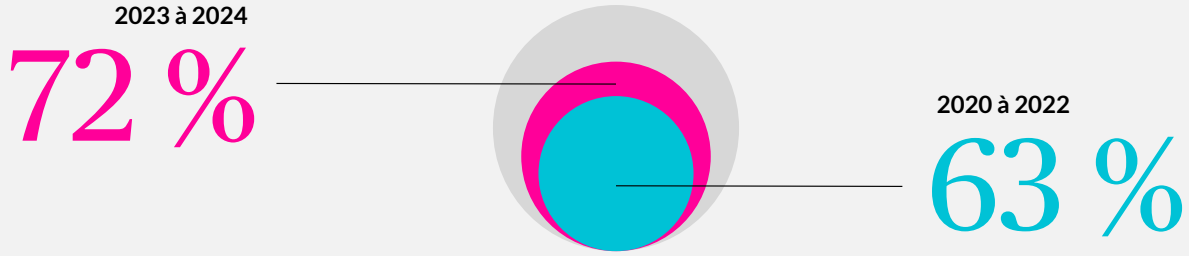
## Pourcentage du nombre total de pertes liées aux cyberincidents déclarées découlant de rançongiciels au cours de l'année civile (États-Unis)



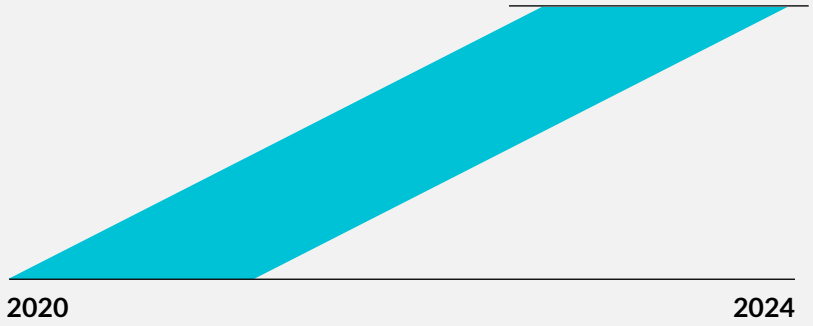

En fin de compte, chaque entreprise faisant face à un rançongiciel doit déterminer ce qui est dans son propre intérêt en prenant en compte de multiples facteurs. Des **ressources sont disponibles**[1] pour les entreprises qui ont raison d'être préoccupées par les risques auxquels elles pourraient faire face et qui cherchent à **maximiser leurs stratégies de défense**[2] in face aux attaquants.

1. Source: https://securityandtechnology.org/ransomwaretaskforce/
2. Source: https://securityandtechnology.org/blog/prepare-dont-pay-a-quick-start-guide-to-defending-against-ransomware/

Les pertes liées aux rançongiciels en 2023 et en 2024 ont représenté près de 72 % du montant des réclamations en matière de cybersécurité, comparativement à une moyenne de 63 % entre 2020 et 2022.



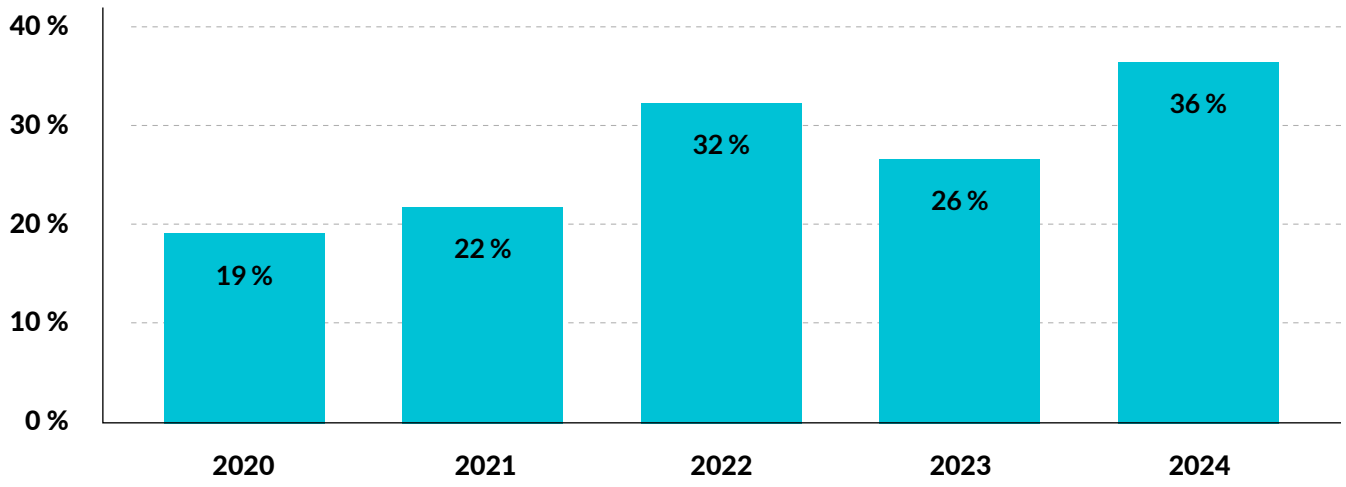

Les incidents liés aux rançongiciels ne doivent pas être considérés comme de simples perturbations pour les clients. Les données compromises, qu'elles soient volées ou diffusées de façon inappropriée, peuvent souvent donner lieu à une poursuite judiciaire ou à un recours collectif, même lorsqu'un client a déployé consciencieusement des contrôles de sécurité. La fréquence des poursuites subséquentes intentées par des tiers découlant d'incidents liés à des rançongiciels en 2024 a augmenté d'environ 75 % par rapport à la moyenne de 2020 à 2021.




Augmentation des poursuites intentées par des tiers découlant de rançongiciels d'environ

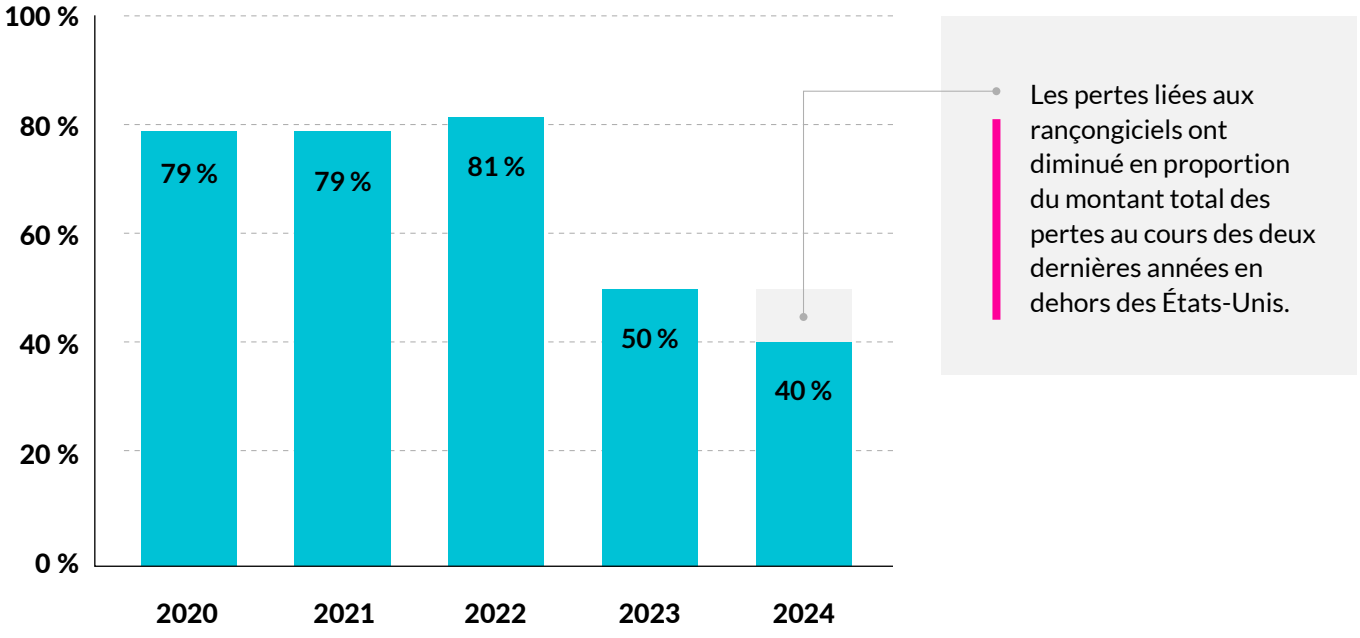
**75 %**

## Proportion de réclamations de tiers en matière de cybersécurité déclenchées par un incident impliquant un rançongiciel (États-Unis)

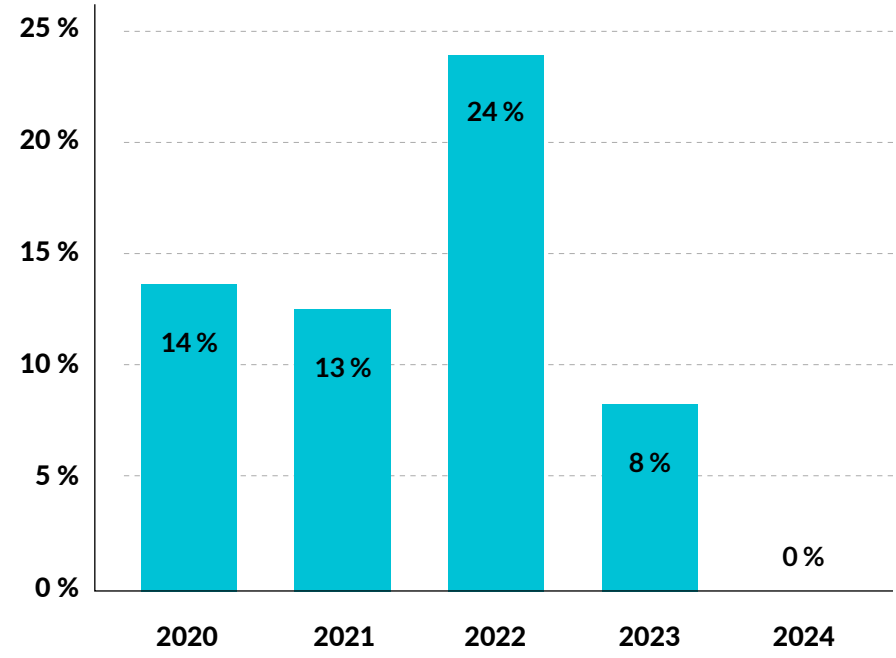


En dehors des États-Unis, cependant, les tendances sont différentes. La proportion de pertes liées aux rançongiciels et la proportion de réclamations de tiers liées aux incidents impliquant des rançongiciels ont diminué au cours des dernières années.

## Pourcentage du nombre total de pertes liées aux cyberincidents déclarées découlant de rançongiciels au cours de l'année civile (hors des États-Unis)

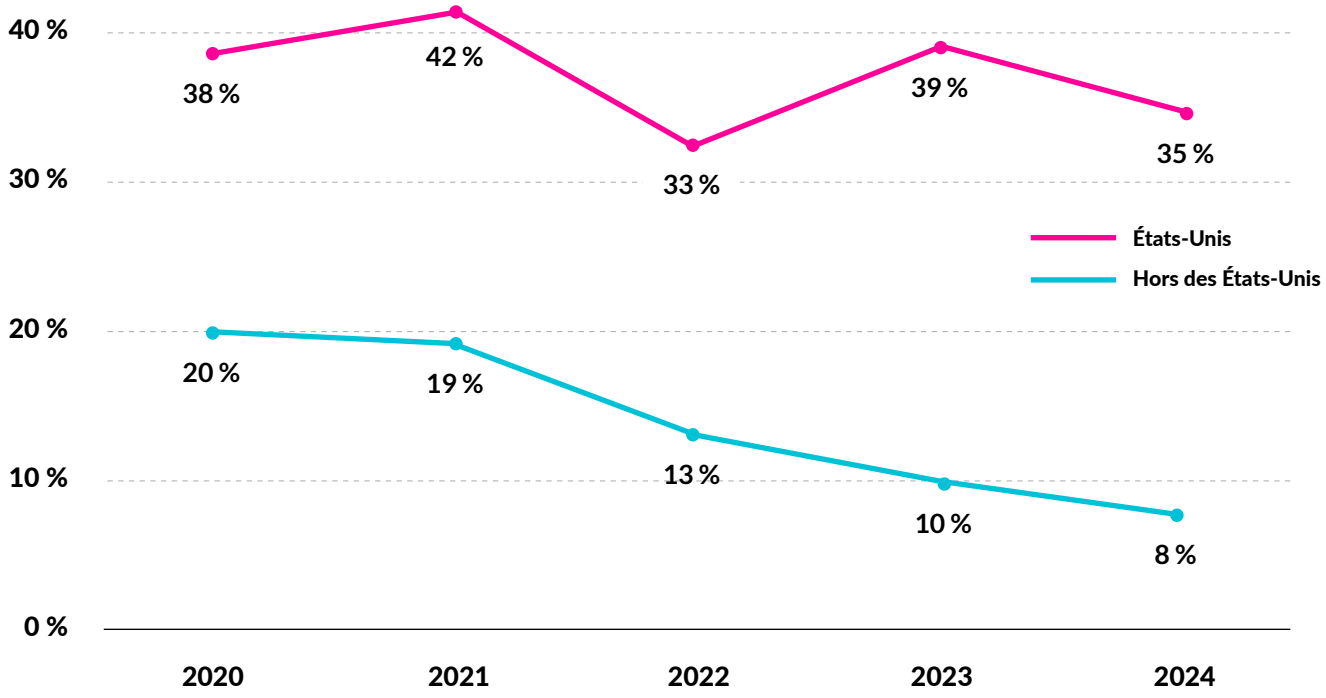



## Proportion de réclamations de tiers en matière de cybersécurité déclenchées par un incident impliquant un rançongiciel (hors des États-Unis)



Nos données indiquent une différence notable entre les assurés aux États-Unis et en dehors des États-Unis en ce qui concerne la volonté de payer des rançons.

## Taux de paiement par rapport aux demandes de rançon




Le taux de paiement par rapport aux demandes de rançon aux États-Unis est considérablement plus élevé qu'en dehors des États-Unis et est resté le même au cours des cinq dernières années.

# Pourquoi un titulaire de police pourrait envisager de payer la rançon

## Considérations économiques

Parfois, le coût du paiement de la rançon est tout simplement inférieur aux pertes financières potentielles qui découleraient des temps d'arrêt et des efforts de récupération des données. Il s'agit d'un calcul rigoureux que de nombreuses entreprises sont obligées de faire.

## Absence d'un environnement de rétablissement viable

Si les sauvegardes de données d'une entreprise sont compromises ou inadéquates, le paiement de la rançon peut être le seul moyen de récupérer l'accès aux données et aux systèmes essentiels. Cela souligne l'importance de solides stratégies de secours et de reprise après sinistre.

## Inquiétudes liées au vol et à l'effacement des données

Les cybercriminels menacent souvent de divulguer ou de supprimer des données volées si la rançon n'est pas payée. Les conséquences potentielles de cette situation, y compris les amendes réglementaires et les poursuites, peuvent être un puissant facteur de motivation au paiement.

## Protection des consommateurs et des partenaires

Dans certains cas, une attaque par rançongiciel peut perturber les services ou compromettre les données des clients ou d'autres entreprises. Le paiement de la rançon peut être considéré comme une façon de minimiser l'incidence sur ces parties prenantes et de maintenir des relations essentielles.

## Acteur de menace très compétent

Si l'attaquant est particulièrement sophistiqué et persistant, celui-ci pourrait causer d'autres dommages ou lancer des attaques subséquentes si la rançon n'est pas payée.

## Situations de vie ou de mort

Dans de rares cas, les attaques par rançongiciel peuvent cibler des infrastructures essentielles ou des fournisseurs de soins de santé, mettant potentiellement des vies en danger. Dans de telles situations, le paiement de la rançon peut être considéré comme la seule option pour éviter une crise humanitaire.

# Pourquoi un titulaire de police pourrait envisager de ne pas payer la rançon

## Sanctions et questions juridiques

Le paiement de rançons à des personnes ou à des entités figurant sur la **liste des sanctions** de l'Office of Foreign Asset Control (OFAC) est illégal. De plus, le financement d'activités criminelles pourrait entraîner des répercussions juridiques ou une atteinte à la réputation.

## Disponibilité de sauvegardes efficaces

Si une entreprise dispose de sauvegardes robustes et testées, elle peut être en mesure de se remettre d'une attaque par rançongiciel sans payer la rançon. Cela souligne l'importance de la sauvegarde des données et des plans de reprise.

## Données qui n'ont pas été compromises

Si l'attaquant n'a pas exfiltré ou chiffré des données sensibles, il peut ne pas être nécessaire de payer la rançon. Toutefois, il est essentiel d'examiner en profondeur l'ampleur de l'attaque pour s'assurer que c'est bien le cas.

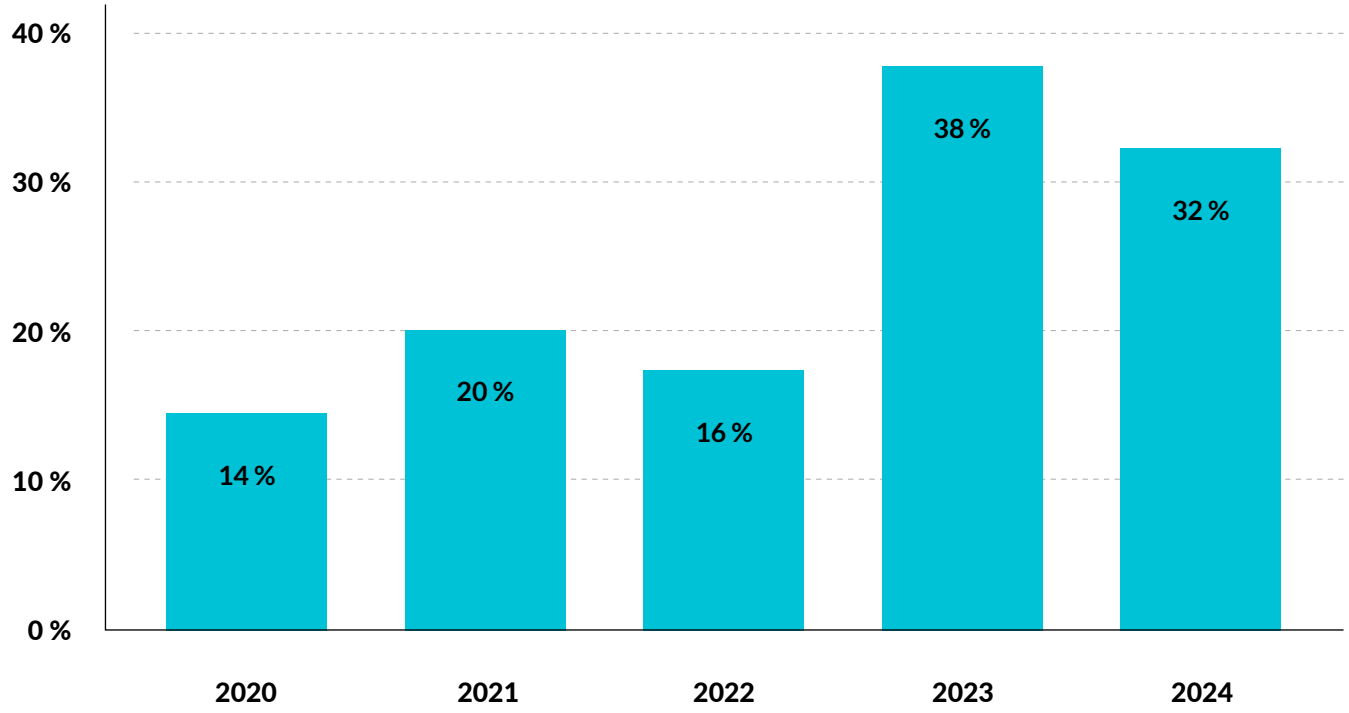
## Question de principe

Certaines organisations peuvent tout simplement refuser de négocier avec les cybercriminels par principe, estimant que le paiement de rançons ne fait qu'encourager de nouvelles attaques.

# La primauté des renseignements personnels

Les problèmes de cybersécurité et de protection des renseignements personnels continuant à se croiser à l'intérieur et à l'extérieur des entreprises, les demandes d'indemnisation se multiplient.

## Proportion de réclamations de tiers en matière de cybersécurité déclenchées par un incident de protection des renseignements personnels (États-Unis)




Aux États-Unis, la proportion de réclamations de tiers liées à la responsabilité en matière de protection des renseignements personnels a doublé en 2023 à 2024 par rapport à la période de 2020 à 2022.

Les polices d'assurance contre les cyberrisques de Chubb couvrent les risques liés à la protection des renseignements personnels de façon plus approfondie que celles de nombreux autres assureurs, en grande partie grâce à notre compréhension approfondie du contexte réglementaire en constante évolution.

## Voici certaines lois américaines qui ont actuellement une incidence considérable sur les réclamations liées à la protection des renseignements personnels :

### Illinois Biometric Information Privacy Act (BIPA)

**Cette loi** réglementant la collecte, l'utilisation et le traitement d'identifiants et d'informations biométriques par des entités privées a entraîné un pic de réclamations qui a commencé en 2019 et qui persiste encore aujourd'hui, à la suite de décisions judiciaires défavorables clarifiant le délai de prescription et l'accumulation des réclamations.

### Video Privacy Protection Act (VPPA)

**Cette loi** concerne directement la manière dont les entreprises utilisent les pixels, ces petits bouts de code intégrés dans un site web qui permettent de suivre une multitude d'événements, notamment les articles qui ont été ajoutés à un panier ou les produits qui ont été examinés au cours d'une visite. Ces renseignements peuvent ensuite être envoyés à un tiers à des fins de publicité ciblée ou à d'autres fins commerciales. Depuis 2022, les assurés de Chubb ont signalé un large éventail de réclamations alléguant que les sites Web ont, par l'entremise de cette activité, divulgué les caractéristiques personnelles identifiables des demandeurs et leur historique de consultation sans leur consentement, en violation de la VPPA. Cette loi prévoit des dommages-intérêts légaux pouvant aller jusqu'à 2 500 dollars par infraction.

### Lois sur le branchement clandestin

Les lois sur le branchement clandestin, telles que le **California Invasion of Privacy Act** (CIPA), permettent aux particuliers d'exercer un droit d'action privé contre les entreprises pour violation de la vie privée, avec des dommages-intérêts légaux pouvant aller jusqu'à 5 000 dollars par violation. D'autres États, comme le Connecticut, le Michigan, la Pennsylvanie et Washington, ont aussi des lois de ce genre. De nombreuses réclamations récentes sont fondées sur la partie de la loi qui interdit explicitement la lecture de tout message, rapport ou communication sans consentement. Les avocats des demandeurs et les tribunaux ont récemment interprété qu'un « message, un rapport ou une communication » peut inclure des renseignements sur les sessions d'un serveur Internet, ce qui signifie que toute tentative faite par une partie pour lire ou apprendre le contenu des renseignements communiqués sur Internet peut légalement constituer de l'écoute clandestine. Les types de réclamations que nous voyons en vertu de cette loi concernent souvent des séances d'analyse et de clavardage sur le Web.

## Aux États-Unis

Les lois et règlements relatifs à la protection des renseignements personnels sont mis en œuvre de plus en plus fréquemment et ont un impact mesurable sur les réclamations, notamment dans les cas d'arbitrage de masse portant sur des violations présumées de la VPPA et des lois sur le branchement clandestin, les frais d'arbitrage devenant payables avant même que le bien-fondé de la demande ne soit examiné. D'autres lois étatiques, comme la **Genetic Information Protection Act** (GIPA) de l'Illinois et la **My Health My Data Act** de l'État de Washington, devraient également être à l'avant-plan des préoccupations des entreprises en matière de responsabilité en matière de protection de la vie privée.

Contrairement à certains de nos pairs, Chubb s'est spécialisée dans la gestion du risque d'atteinte involontaire aux renseignements personnels. Nos spécialistes des réclamations en matière de cybersécurité peuvent aider les entreprises à éviter les litiges en partageant nos connaissances sur les questions juridiques et technologiques pertinentes, des questions qui ne feront que s'aggraver à mesure que des facteurs comme l'intelligence artificielle déloyale entreront en jeu.

## En dehors des États-Unis

En dehors des États-Unis, d'autres cadres tels que la **Loi canadienne sur la protection des renseignements personnels et les documents électroniques (LPRPDE)** et le **Règlement général sur la protection des données (RGPD)** de l'UE réglementent la collecte, le traitement, l'utilisation, la conservation et la suppression licites des renseignements personnels identifiables. Compte tenu des préoccupations croissantes concernant la façon dont les données personnelles sont partagées à l'échelle mondiale à des fins commerciales, de nombreux pays ont élaboré ou sont en train d'élaborer des lois qui peuvent créer des obligations et des risques pour toutes les entreprises qui font des affaires à l'échelle internationale, et pas seulement pour les entreprises médiatiques.

# Les contrôles sont importants - Adopter un modèle à vérification systématique en matière de cybersécurité

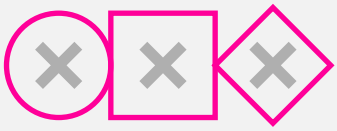
Les événements systémiques ne sont pas toujours le résultat d'une attaque malveillante. En juillet 2024, **CrowdStrike**, une entreprise américaine de cybersécurité, a envoyé une mise à jour logicielle défectueuse à des clients partout dans le monde qui a touché spécifiquement les postes de travail et les serveurs. Des milliers d'entreprises qui utilisaient CrowdStrike ont été touchées, et des milliers d'autres ont été touchées parce que leurs fournisseurs utilisaient CrowdStrike.

Cet incident a causé des perturbations mondiales.

**8,5 millions**

**de systèmes sont tombés en panne**

Tant les clients directs de CrowdStrike que ceux dont les fournisseurs utilisaient CrowdStrike ont été touchés.



Les compagnies aériennes, les hôpitaux, les banques, les marchés boursiers, les gouvernements, les commerces de détail et bien d'autres qui

**400 M$ à 1,5 G$**

**en pertes assurées**

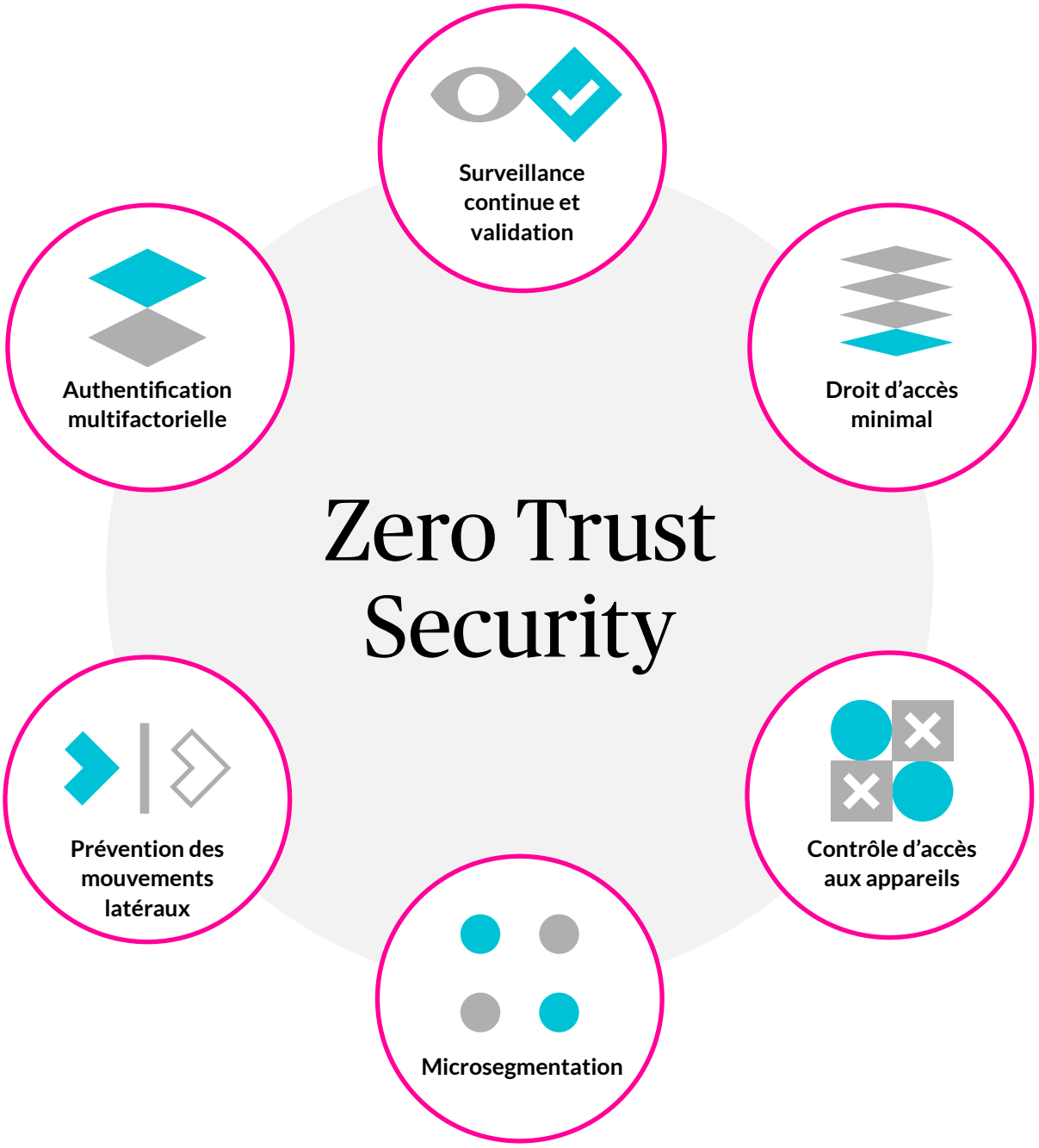
Les clients ayant mis en place des mesures de résilience solides ont été moins touchés.

Source: https://www.cybcube.com/news/cybercube-estimates-global-insured-losses-from-crowdstrike-event#:~:text=The%20faulty%20CrowdStrike%20Falcon%20Sensor,premiums%20of%20$15bn%20today

La panne de CrowdStrike a rappelé que les incidents non malveillants peuvent avoir autant d'impact que les cyberattaques malveillantes. Les leçons pratiques qui peuvent être tirées de cet événement malheureux comprennent l'importance de mettre en œuvre et de répéter des plans d'intervention en cas d'incident, ainsi que d'utiliser des mesures de résilience pour atténuer les événements imprévus qui ont une incidence directe sur votre entreprise ou sur votre chaîne d'approvisionnement et s'en remettre rapidement.

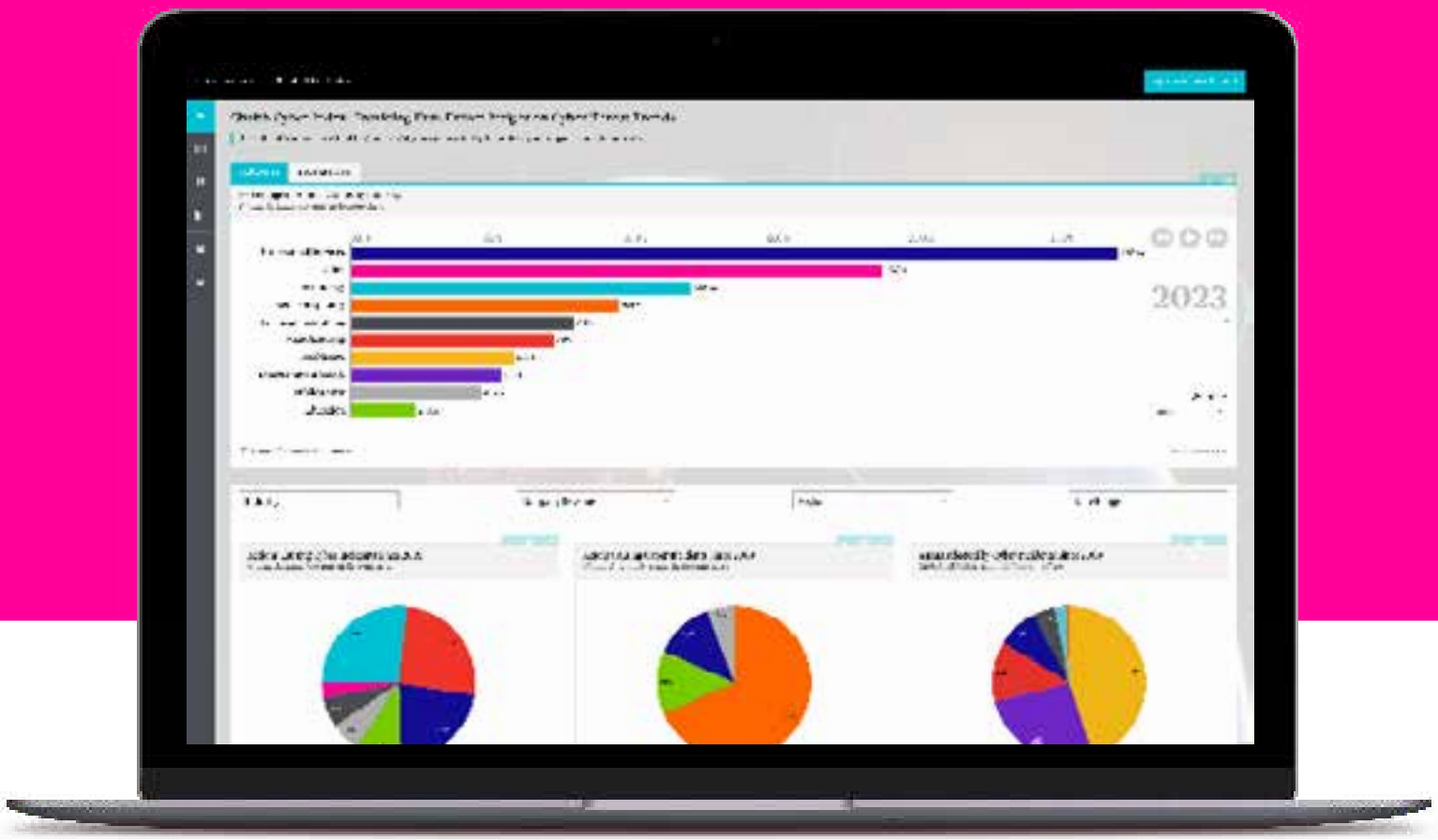
## Un **modèle de sécurité à vérification systématique** est essentiel pour maintenir les contrôles.

Cela signifie qu'il faut employer et maintenir des protocoles stricts qui minimisent le risque d'infractions, de perturbations, d'infections ou d'erreurs en exigeant les vérifications d'identité les plus rigoureuses pour chaque personne qui tente d'accéder à un réseau privé – indépendamment de son emplacement ou de son statut au sein de l'organisation. Les outils et les politiques pourraient inclure **l'authentification multifactorielle**,[1] le **principe de droit d'accès minimal**[2] et la **microsegmentation du réseau**,[3] parmi d'autres solutions qui ont démontré qu'elles réduisaient considérablement le risque.




1. Source: https://www.cisa.gov/MFA
2. Source: https://www.techtarget.com/searchsecurity/definition/principle-of-least-privilege-POLP
3. Source: https://www.cisco.com/c/en/us/products/security/what-is-microsegmentation.html

# L'outil Cyber Index de Chubb : Renforcer les entreprises grâce à des informations fondées sur des données




The **Cyber Index de Chubb** est un outil numérique qui permet aux utilisateurs d'accéder à nos données exclusives concernant les cybermenaces et d'élaborer des stratégies pour se protéger. Il continue de se développer et d'informer nos courtiers, en fournissant des informations précieuses sur les tendances et les risques cybernétiques spécifiques au secteur. La richesse des données qu'il contient alimente nos décisions de souscription, ce qui nous permet d'offrir des solutions sur mesure à nos clients.

# Consultez l'outile Cyber Index de Chubb pour découvrir et utiliser :

## Des informations spécifiques à l'industrie

Une ventilation détaillée des tendances et des répercussions des cyberattaques dans divers secteurs et pour diverses tailles de revenus – qui peut être filtrée par date ou par région – permettant aux entreprises de comparer leur profil de risque à celui de leurs pairs.

## Les coûts des réclamations et les coûts payés de la réponse aux incidents pour les cyber-événements

Les moyennes sectorielles depuis 2009.

## L'évaluation de la vulnérabilité aux rançongiciels

Un outil spécialisé, sous la forme d'un questionnaire, qui permet aux entreprises et aux organisations d'identifier leurs vulnérabilités uniques aux attaques par rançongiciel et de jeter les bases de stratégies défensives.

## Calculateur de risques cybernétiques

Permet aux utilisateurs d'avoir une meilleure idée de l'éventail plus large des cyberrisques et des coûts potentiels auxquels ils pourraient être exposés.

## Perspectives d'achat par les pairs

Permet aux utilisateurs d'examiner les décisions prises par d'autres entreprises ou organisations en matière de cyberprotection; peut être ventilé par secteur d'activité, par région et par chiffre d'affaires.

## Bibliothèque et glossaire

Liens vers des vidéos et des balados, ainsi que d'autres références pour aider les entreprises et les organisations à explorer davantage le paysage en constante évolution de la cybersécurité.

# Aider les entreprises à devenir plus sûres

Les entreprises n'ont peut-être pas les ressources nécessaires pour lutter seules contre les cyberincidents sur tous les fronts.

Parmi les nombreux **services de gestion des risques** que nous offrons à nos clients figure **l'Ensemble de services Cyber de Chubb**, conçu spécialement pour les entreprises de 100 employés ou moins. Ce service relie ces entreprises directement à l'équipe de Cyberconseillers de Chubb et les aide à élaborer les stratégies de gestion et d'intervention les plus efficaces.

## Quelle que soit la taille de votre entreprise, Chubb peut offrir des solutions novatrices en assurance contre les cyberrisques.

Chubb est le partenaire principal et la ressource de référence pour les entreprises de toutes tailles qui recherchent une cyberprotection. Travaillez avec notre équipe de cyberconseillers pour protéger votre organisation des pertes financières et de réputation liées à la cybersécurité, et pour avoir accès à des outils d'atténuation et à des ressources-conseils essentiels qui peuvent aider à réduire votre exposition 365 jours par année. Pour en savoir plus, cliquez sur le code QR ci-dessous.

Ce ne sont là que quelques-uns des outils que Chubb offre pour atteindre notre objectif d'aider les clients à se protéger contre les cyberincidents coûteux et à renforcer continuellement leurs

CHUBB®

chubb.com