CHUBB®

Maîtriser la dynamique du risque :

Intelligence artificielle, contentieux et résilience

Rapport 2026 sur les sinistres cyber

Section 1

Introduction : Divergence

La nature du risque cyber ne cesse d'évoluer, tandis que l'étendue des vulnérabilités et l'exposition au risque s'accroissent. Portés par la bonne intégration de systèmes de détection pilotés par l'IA et par une résilience renforcée, plusieurs marchés mondiaux ont vu la fréquence des incidents cyber se stabiliser en 2025, selon des rapports récents. Les États-Unis, eux, ont atteint un niveau historique de gravité, le coût moyen d'une violation de données en 2025 **dépassant 10,2 millions de dollars** – soit plus du double de la moyenne mondiale de 4,4 millions de dollars.

Au bout du compte, la réussite de toute entreprise – ou de tout marché géographique – pour se protéger des incidents cyber repose sur une bonne compréhension d'un paysage de menaces en constante évolution, des cadres juridiques et réglementaires qui encadrent ses activités de collecte et de stockage des données, ainsi que de l'interdépendance des partenaires commerciaux, qui accroît l'exposition tout au long de la chaîne d'approvisionnement d'une entreprise.

Cette édition du rapport Chubb Cyber Claims analyse les données historiques de sinistres de Chubb jusqu'à décembre 2025 afin de mettre en lumière les tendances de fréquence et de gravité des sinistres – ainsi que les facteurs qui alimentent ces évolutions – pour aider les entreprises à évoluer dans un environnement de risque cyber complexe et à renforcer leur résilience financière et opérationnelle.

Source : *Rapport IBM 2025 sur le coût d'une violation de données*

Section 2

Tendances mondiales des sinistres

Sur l'ensemble des marchés, la hausse des sinistres cyber a été alimentée par l'évolution des technologies et du cadre juridique, ainsi que par l'interdépendance des chaînes d'approvisionnement. Trois tendances se distinguent :

01

L'IA accélère la vitesse du risque.

La même technologie d'IA qui a permis une détection plus rapide et plus approfondie des incidents cyber a profondément modifié leur rythme : en intégrant une IA agentique et autonome aux malwares, des acteurs malveillants parviennent désormais à compromettre plusieurs systèmes en l'espace de quelques minutes – ne laissant quasiment plus de marge pour une intervention manuelle. L'usage d'IA avancées, comme les grands modèles de langage (LLM), progresse à un rythme presque identique à l'adoption de l'IA par le grand public.

02

Le réflexe « contentieux d'abord ».

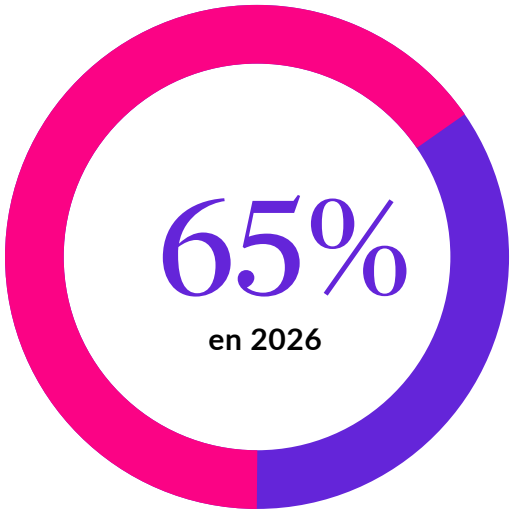
Un incident cyber n'est plus seulement une défaillance technique à corriger: il déclenche fréquemment une action en justice peu après les faits. Au cours des 30 dernières années, les lois sur la vie privée et la protection des données ont été adoptées à un rythme exceptionnel, rendant la conformité plus complexe et multipliant les contentieux liés à la confidentialité. L'intervalle entre une violation et le premier recours collectif s'est réduit, les procédures étant souvent engagées en quelques jours, avec des griefs variables, quelle que soit la taille de l'entité ou les contrôles jugés insuffisants.

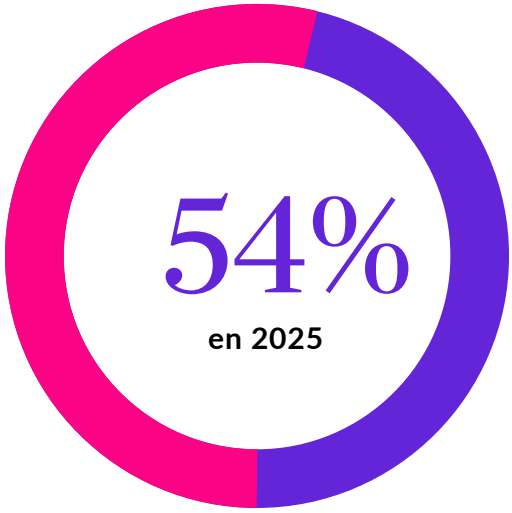
03

Interdépendance systémique.

Il y a encore quelques années, les responsables des risques se concentraient surtout sur la prévention de leurs propres défaillances cyber, afin qu'elles n'affectent pas leurs clients et leurs fournisseurs. Aujourd'hui, la prise de conscience est largement partagée quant au poids que la chaîne d'approvisionnement de l'organisation peut avoir sur la fréquence et la gravité des incidents cyber.

Selon le World Economic Forum, 65% des grandes entreprises considèrent aujourd'hui les vulnérabilités des tiers et de la chaîne d'approvisionnement comme leur principal défi en matière de cybersécurité — contre 54% en 2025.





Un incident cyber chez un constructeur automobile mondial

Comme nous le détaillerons plus loin, des événements tels que l'Incident cybernétique d'août 2025 touchant un grand constructeur automobile mondial ont mis en évidence l'ampleur des répercussions économiques et opérationnelles qu'un incident cyber peut provoquer à n'importe quel niveau d'une chaîne d'approvisionnement. L'événement a provoqué une onde de choc dans l'ensemble de l'économie britannique, avec des effets massifs et immédiats. Outre les pertes financières considérables subies par le constructeur en raison des arrêts de production, il doit désormais faire face à de nombreuses actions collectives liées à cet incident.

Section 3

Fréquence et gravité des incidents cyber

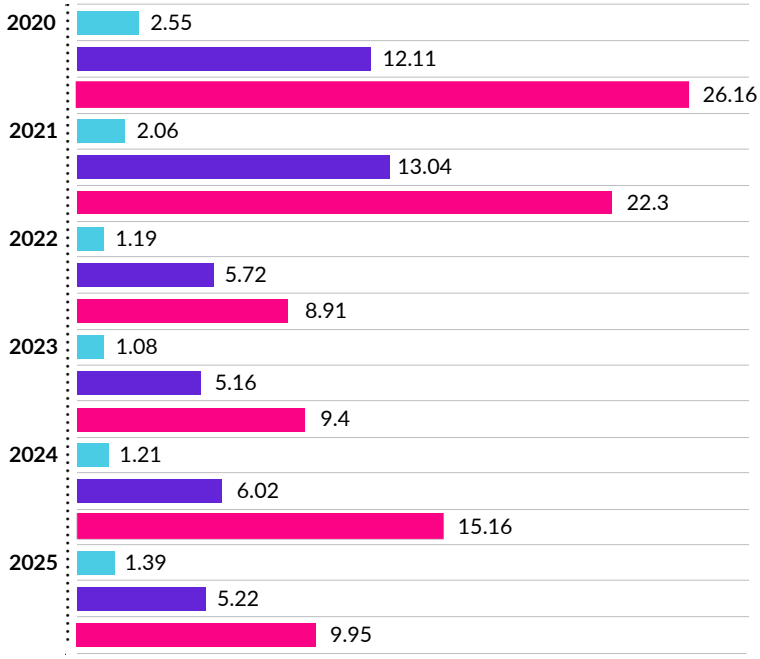
La fréquence, c'est-à-dire le nombre de sinistres par police, et la gravité, soit le coût moyen par sinistre, constituent les principaux déterminants du coût des sinistres en assurance et les principaux facteurs d'évolution des primes. Comme, par nature, l'assurance est une activité où la prime facturée arrive après le coût réel des sinistres, les tendances récentes de la fréquence et de la gravité servent d'indicateur avancé des tarifs de l'année à venir.

Les tableaux ci-contre présentent une image contrastée des tendances de fréquence et de sévérité au sein du paysage cyber aux États-Unis sur les six dernières années.

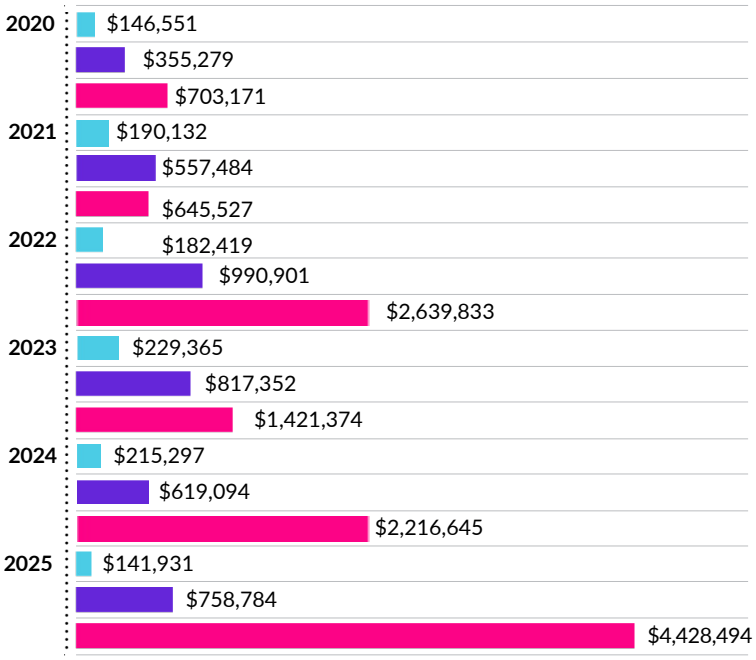
Les progrès réalisés dans les profils de sécurité et les capacités de résilience des clients se traduisent par une baisse marquée de la fréquence des sinistres, tous secteurs et tailles d'entreprises confondus, entre 2020 et 2022. Parallèlement, les données montrent une hausse globale de la fréquence au sein des petites et moyennes entreprises (PME) et des portefeuilles de grands risques depuis 2022, tandis que le segment mid-market est resté plus stable sur la même période.

Le déploiement des limites a reculé depuis 2021, alors même que la sévérité a augmenté. Si la sévérité est restée stable dans le segment PME, elle a nettement progressé sur le mid-market et encore plus fortement sur le segment des grands comptes. Plusieurs facteurs expliquent cette hausse, notamment l'augmentation des coûts liés aux interruptions d'activité et la montée des dépenses de contentieux, tant pour les violations de données que pour les atteintes à la vie privée.

Fréquence des sinistres cyber pour 100 polices (États-Unis)



Sévérité moyenne des sinistres cyber (États-Unis)



PME : chiffre d'affaires de $0 à $99M

Marché intermédiaire : chiffre d'affaires de $100M à $999M

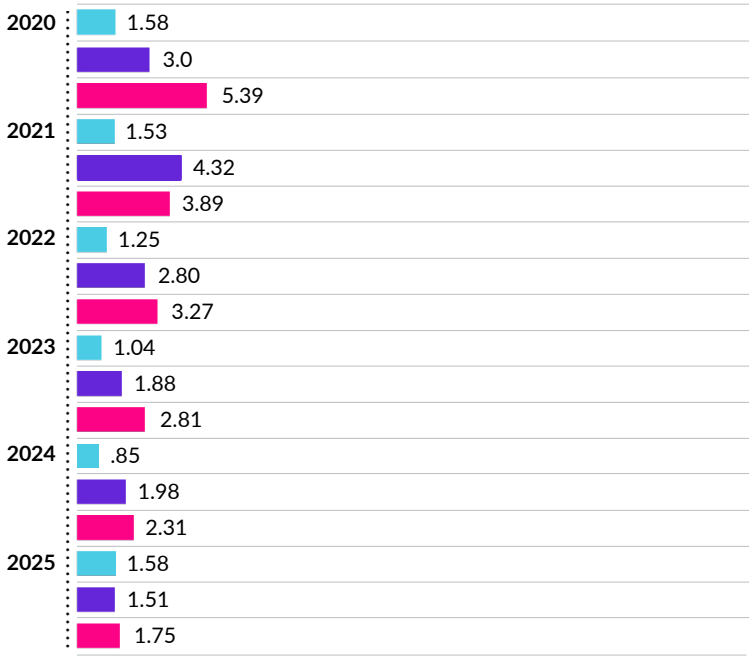
Grandes entreprises : chiffre d'affaires d'$1B+

Tendances en Europe et au Royaume-Uni: entre points communs et écarts par rapport aux États-Unis.

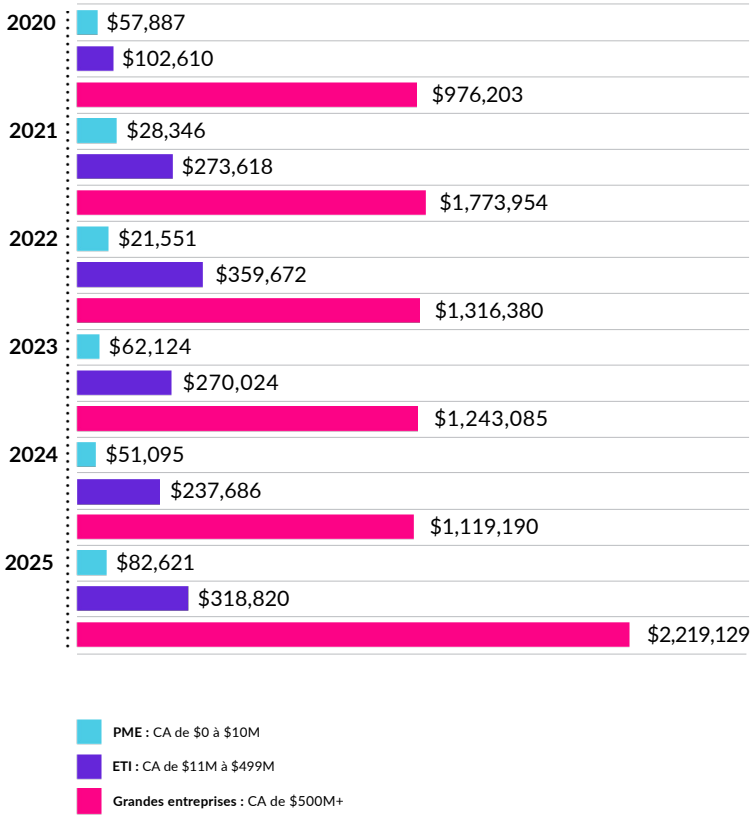
Les niveaux de fréquence sont comparables pour la cohorte PME, mais nettement plus faibles pour les segments du mid-market et des grands comptes. Cela laisse penser que la probabilité d'être ciblé, ainsi que le profil de sécurité global et les contrôles en place, sont similaires parmi les PME aux États-Unis, en Europe et au Royaume-Uni. En revanche, l'exposition recule clairement pour les entreprises de taille intermédiaire et les grandes entreprises en Europe et au Royaume-Uni par rapport aux États-Unis – principalement en raison de l'absence de réclamations liées à des litiges intentés par des tiers.

La gravité est plus faible pour l'ensemble des cohortes en Europe et au Royaume-Uni, là encore principalement du fait de l'absence de frais significatifs de contentieux engagés par des tiers, qu'il s'agisse de violations de données ou de réclamations relatives à la vie privée sans violation de données. Si la gravité progresse nettement dans toutes les cohortes, elle reste plus stable qu'aux États-Unis.

Fréquence des sinistres cyber pour 100 polices (Europe + Royaume-Uni)



Sévérité moyenne des sinistres cyber (Europe + Royaume-Uni)



PME : CA de $0 à $10M

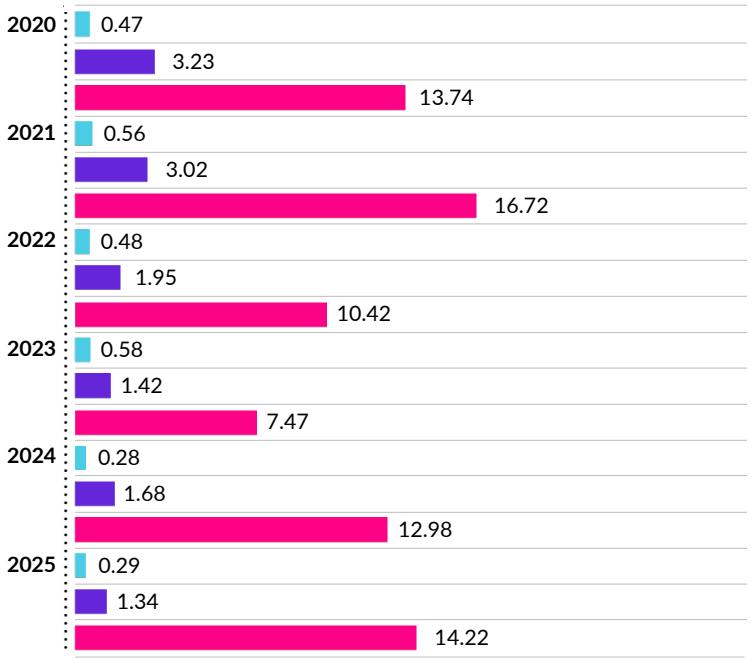
ETI : CA de $11M à $499M

Grandes entreprises : CA de $500M+

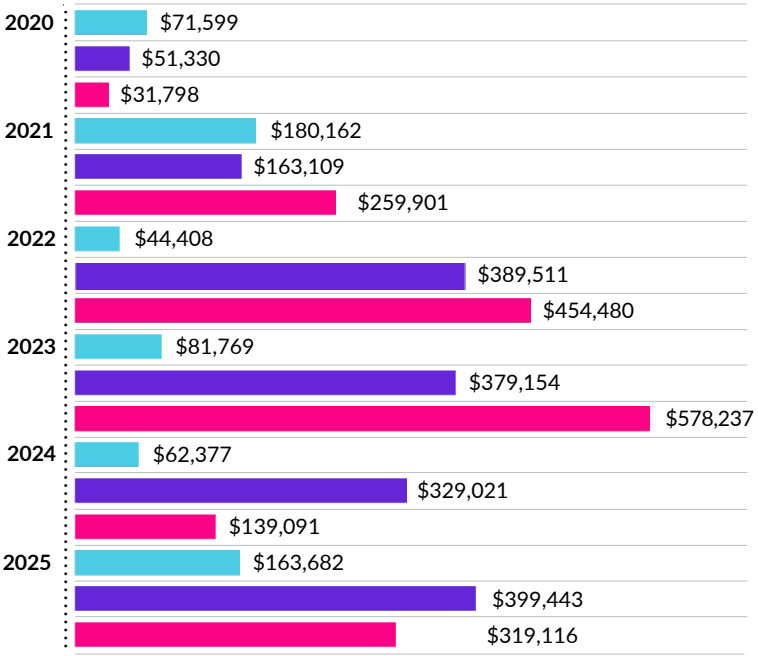
En Australie et en Nouvelle-Zélande, les niveaux absolus de fréquence et de gravité, ainsi que les tendances globales, diffèrent de ceux observés dans d'autres régions du monde, tout en suivant la même dynamique générale.

La fréquence a nettement reculé, tandis que la gravité a globalement augmenté après 2021. La fréquence des sinistres des PME ne représente qu'une fraction des niveaux observés ailleurs dans le monde, alors que la gravité est globalement comparable. La fréquence sur le segment « middle market » est proche de celle de l'Europe et du Royaume-Uni – et bien inférieure à celle des États-Unis – ce qui reflète un cadre juridique relativement favorable en matière d'actions liées aux violations de données et aux atteintes à la vie privée sans fuite de données. À noter également : les segments « middle market » et grandes entreprises ont affiché des niveaux de gravité plus faibles, avec des hausses plus modérées au fil du temps.

Fréquence des sinistres cyber pour 100 polices (Australie & Nouvelle-Zélande)



Sévérité moyenne des sinistres cyber (Australie & Nouvelle-Zélande)



PME : $0-$10M de chiffre d'affaires

Entreprises de taille intermédiaire : $11M-$499M de chiffre d'affaires

Grandes entreprises : $500M+ de chiffre d'affaires

Section 4

La course aux armements de l'IA : attaque et défense

L'adoption croissante et les progrès de l'IA à l'échelle mondiale ont entraîné un usage malveillant de plus en plus sophistiqué, tout en faisant émerger des outils de détection et de remédiation bénéfiques.

En outre, des incidents liés à l'IA, moins sophistiqués, se poursuivent, par exemple lorsqu'un salarié téléverse par erreur des données personnelles (PII) dans un LLM accessible au public, ce qui déclenche un incident cyber.

Côté défense, les entreprises et les organisations peuvent mettre en place des outils éprouvés de réduction des risques, centrés sur l'IA, pour faire face à ces menaces et limiter leur exposition.

Parmi ces mesures :

Défenses « AI-First » : Adopter des opérations de sécurité pilotées par l'IA (AISO) pour détecter les menaces en temps réel.

Gouvernance de l'IA :
Tenir un inventaire rigoureux de tous les systèmes d'IA et auditer les pratiques de traitement des données des prestataires.

Formation renforcée : Sensibiliser les collaborateurs aux risques de sécurité liés à l'IA, comme le phishing avancé et les deepfakes.

Section 5

L’impact de la fraude par ingénierie sociale

Les déclarations de sinistres liées à l’ingénierie sociale peuvent être lourdes de conséquences – surtout pour les petites et moyennes entreprises. Les risques de pertes financières, de perturbations opérationnelles et d’atteinte à la réputation soulignent l’urgence de mettre en place des stratégies efficaces de réponse et de rétablissement.

Incident cyber de fraude par ingénierie sociale

L'événement : Suite à un e-mail semblant provenir d'un représentant d'un fournisseur de machines de longue date, une nouvelle recrue modifie les coordonnées bancaires du paiement du fournisseur au profit d'une nouvelle banque, sans chercher d'abord à vérifier l'e-mail en appelant le fournisseur à son bureau.

L'impact : L'entreprise se rend compte par la suite que l'employé a été victime d'une fraude par ingénierie sociale lorsque le véritable salarié du fournisseur relance pour le paiement, découvrant alors que l'e-mail était frauduleux et que le règlement avait été effectué au profit d'un usurpateur.

100 000 $

La solution : Perte de plus de $100,000. Aucun remboursement de la banque ni du fournisseur.

Le résultat : La police cyber, avec une extension « cybercriminalité », indemnise l'assuré pour les pertes non récupérables.

Section 6

La nouvelle frontière de la vie privée & le réflexe « contentieux d'abord »

À mesure que les incidents cyber deviennent de plus en plus des affaires juridiques, les entreprises doivent relever de nouveaux défis liés à des théories inédites de responsabilité — notamment autour de l'écoute clandestine et des technologies de suivi numérique.

Principaux facteurs influençant la responsabilité juridique :

Le réflexe contentieux d'abord :
Aux États-Unis, les avocats des plaignants s'appuient sur des lois d'écoute téléphonique vieilles de plusieurs décennies (comme la California Invasion of Privacy Act) et sur des textes relatifs à la confidentialité des vidéos (comme la loi fédérale Video Protection Privacy Act) pour viser des technologies web courantes, dont l'usage de pixels de suivi.

Législation sur les données et la vie privée : L'évolution des règles de confidentialité au Royaume-Uni et en Europe, **le Règlement général sur la protection des données (RGPD)** et la **loi sur l'utilisation et l'accès aux données de 2025 (DUAA)**, qui s'appuie sur la loi britannique sur la protection des données, a entraîné des obligations complexes pour les entreprises lorsqu'elles traitent des données personnelles, y compris l'usage de technologies web courantes, comme les pixels de suivi.

Arbitrage de masse : Aux États-Unis, les entreprises sont contraintes de payer d'importants frais administratifs initiaux pour chaque dépôt individuel. Dans une action impliquant 10 000 plaignants, par exemple, ces frais non remboursables peuvent dépasser 10 millions de $ avant même que le fond du dossier ne soit examiné.

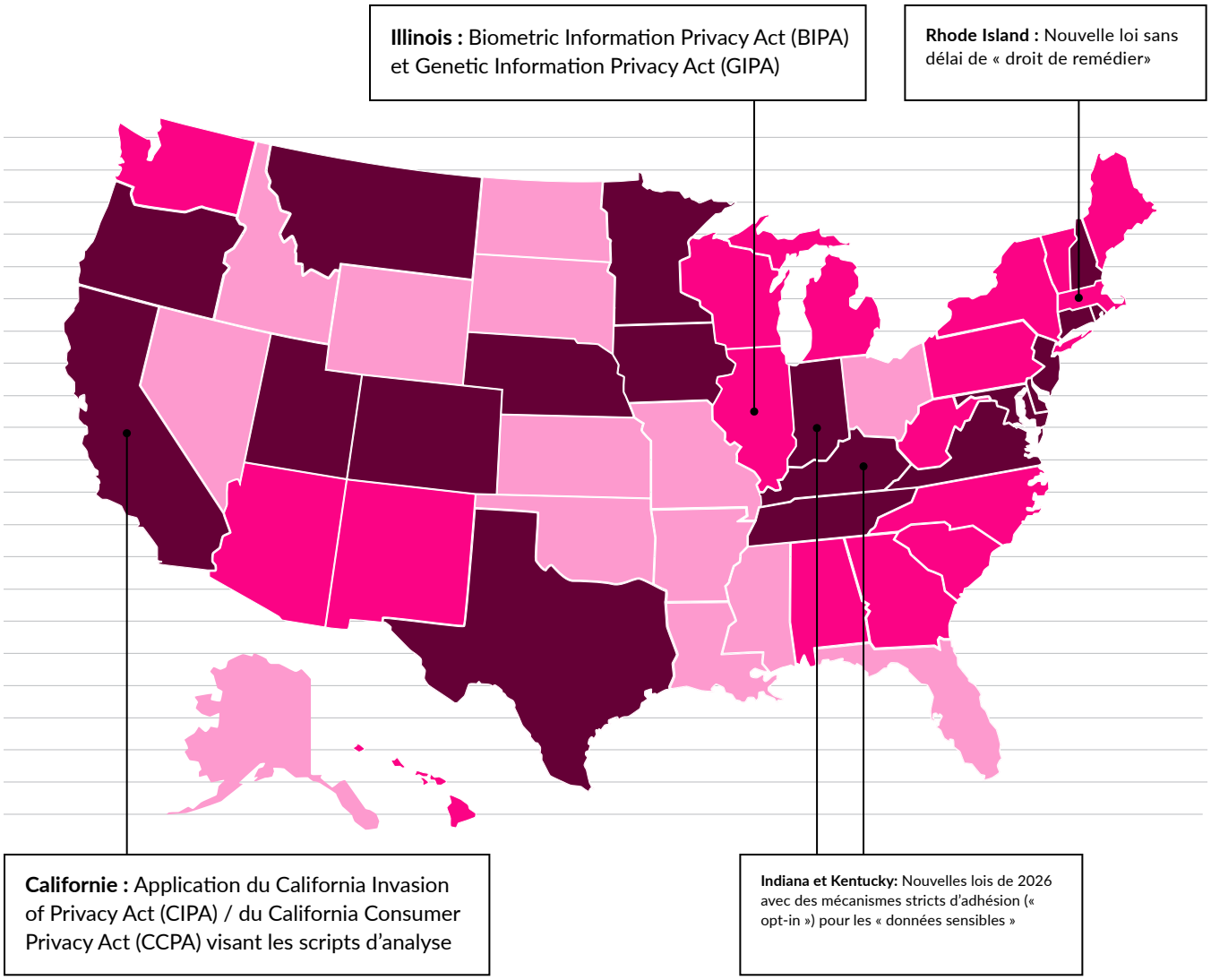
Suppression de données : Les attaquants tendent de plus en plus à supprimer volontairement des données ou à les divulguer, plutôt que de se contenter de les chiffrer — entraînant une « perte de contrôle » durable — ce qui peut alourdir les enjeux en cas de contentieux.

Un nombre croissant de lois sur la protection de la vie privée aux États-Unis et dans l'UE imposent des obligations complexes et à plusieurs niveaux aux entreprises qui stockent et/ou transfèrent des données personnelles. Cela inclut le droit de refuser le profilage ou la prise de décision automatisée, des exigences de transparence pour les traitements pilotés par l'IA, et des évaluations des risques obligatoires pour les cas d'usage à haut risque.

États-Unis

Suivi des lois sur la protection des données

Il n'existe pas de loi fédérale ; la réglementation forme plutôt un patchwork, État par État.



Source : *Suivi de la législation fédérale américaine sur la protection de la vie privée*

Texte de loi / projet en cours d'examen :

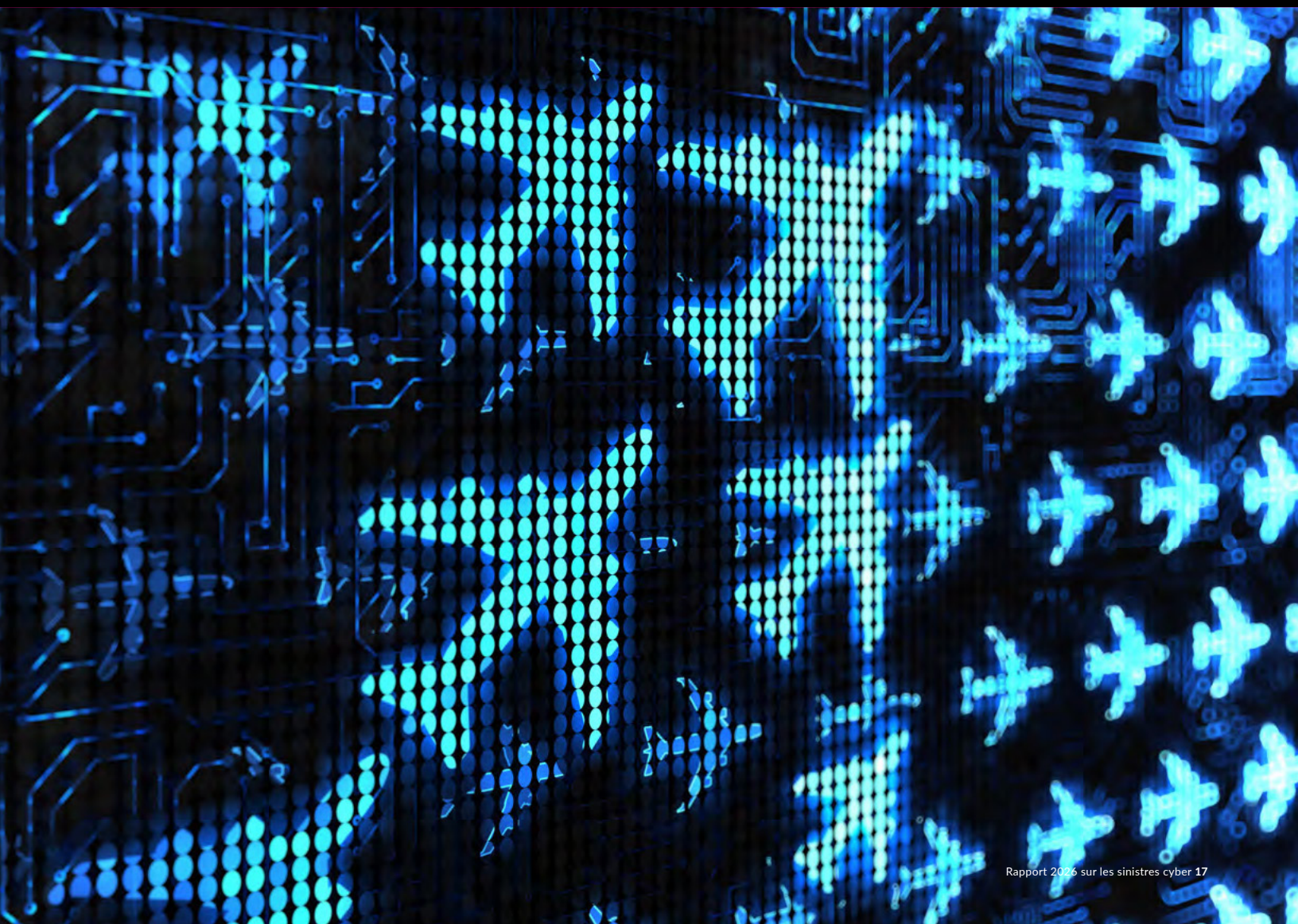
Législation adoptée **Législation en attente** **Aucune législation**

Pour les entreprises au Royaume-Uni et en Europe, il est important de tenir compte du patchwork de réglementations propres à chaque État lorsqu'elles commercent avec les États-Unis ou y exercent. Pour en savoir plus, rendez-vous sur **Chubb Cyber Insurance**.

Section 7

Protection des données sensibles

Les incidents liés à la vie privée alimentent de plus en plus des sinistres cyber à la fois fréquents et lourds. Avec l'évolution des réglementations et la montée des contentieux de grande ampleur, la gestion du risque de confidentialité est devenue plus complexe et plus coûteuse. Chaque organisation peut se heurter à des défis spécifiques pour protéger ses données dans un paysage de menaces en perpétuelle évolution.



Marché intermédiaire
Incident de confidentialité

L'événement : L'assuré exploite un site web par abonnement et une application mobile utilisant des technologies de suivi, notamment des cookies et des pixels. Le pixel collecte certaines données, dont l'identifiant utilisateur du site, et les transmet à des tiers.

L'impact : Plusieurs cabinets d'avocats ont adressé des milliers de mises en demeure avant arbitrage, alléguant que l'utilisation du pixel enfreignait le California Invasion of Privacy Act, qui interdit l'interception de communications sans consentement.

+40M$

Le problème : La politique de confidentialité de l'assuré imposait que tout litige soit réglé par arbitrage. Or, selon le règlement de l'organisme d'arbitrage, l'assuré aurait dû avancer plusieurs millions de dollars de frais de dépôt dès l'ouverture du dossier, avant même d'examiner le bien-fondé des demandes. Ainsi, si les réclamations avaient été arbitrées, cela aurait pu entraîner une condamnation potentielle à des dommages-intérêts légaux, à laquelle se seraient ajoutés des frais d'arbitrage, pour un total dépassant $40 million.

La solution : Chubb a mandaté un conseil rompu aux contentieux liés à la confidentialité, ainsi qu'aux échanges avec ces cabinets, ce qui a conduit à une médiation du litige.

6,5M$

Le résultat : L'ensemble des réclamations a fait l'objet d'un règlement global autour de 6,5 M$.

Maîtriser les risques liés à la confidentialité des consommateurs et garantir la conformité réglementaire est essentiel. Pour accompagner nos assurés, Chubb s'est associé à des plateformes de gestion des risques de confidentialité qui permettent aux assurés de protéger leur organisation en évaluant et en gérant de manière proactive les risques de confidentialité, en sécurisant les données sensibles et en maintenant la conformité.

Section 8

L’impact des rançongiciels sur les petites et moyennes entreprises

Les attaques par rançongiciel continuent de faire peser des risques majeurs sur les petites et moyennes entreprises (PME), entraînant souvent des violations de données complexes et coûteuses. Même lorsque les premières tentatives de chiffrement sont déjouées, l’exfiltration d’informations sensibles peut imposer de vastes obligations de notification et des efforts de remédiation.

Incident de rançongiciel (PME)

L'événement : Les tentatives d'un groupe de cybercriminels visant à chiffrer l'ordinateur de l'assuré ont été largement déjouées par l'outil de détection et de réponse sur les terminaux (EDR) de l'assuré. Toutefois, l'attaquant est parvenu à exfiltrer des informations de santé ainsi que les numéros de sécurité sociale de plus de 4 millions de personnes.

L'impact : L'assuré devait identifier rapidement et avec précision quelles données et quelles informations de santé à caractère personnel avaient été compromises afin de respecter les obligations de notification prévues par les lois et réglementations applicables.

Le problème : Évaluer l'ampleur de la violation de données, notifier rapidement les personnes concernées et traiter au plus vite les vulnérabilités non corrigées, encore exploitables par un tiers malveillant.

4M$

La solution : Un cabinet d'avocats, une équipe de forensique et une équipe d'analyse de données ont été mobilisés sans délai pour accompagner l'assuré dans la gestion de cet incident. Après une analyse approfondie des données concernées, 4 millions de personnes ainsi que de nombreux régulateurs ont été informés de l'incident. L'équipe Risk Advisor de Chubb a également été sollicitée pour aider le client à traiter ses vulnérabilités non corrigées.

4,7M$

Le résultat : Le coût total remboursé à l'assuré s'est élevé à $4.7 millions, dont $2.4 millions de frais de notification et$1.2 million de coûts de surveillance du crédit pour les victimes. L'assuré a également été alerté de ses vulnérabilités non corrigées et accompagné dans leur remédiation.

Chubb dispose d'une solide expérience en matière de sinistres liés aux rançongiciels et propose des services juridiques, d'investigation informatique, de relations publiques et d'autres expertises spécialisées pour aider nos assurés à réagir et à gérer sereinement les incidents de rançongiciel : réparer ou remplacer les systèmes endommagés, réduire les interruptions, et reprendre l'activité.

Section 9

Rançongiciel sans frontières

Les attaques par rançongiciel continuent de faire peser de graves risques sur les organisations du monde entier. Même les institutions dotées de mesures de cybersécurité avancées peuvent subir d'importantes perturbations lorsque des acteurs malveillants exfiltrent des données sensibles et les diffusent publiquement. Les répercussions dépassent souvent les frontières, entraînant une surveillance réglementaire accrue, des obligations juridiques et des défis opérationnels.

Comme le montre cet incident en Europe, les rançongiciels ne connaissent aucune frontière géographique.

Incident mondial de rançongiciel

L'événement : Une attaque par rançongiciel menée par un groupe d'attaquants encore inconnu à l'époque a visé une institution universitaire internationale et sa branche d'édition. Plus de 575 000 documents sensibles ont été exfiltrés, puis publiés sur le site de fuite du groupe.

L'impact : Les opérations ont été perturbées à l'échelle mondiale. Des données sensibles, dont les revenus des auteurs, des recherches gouvernementales et des sujets d'examens à venir, ont été exposées dans plus de 40 pays. Le rétablissement a été particulièrement difficile dans les régions aux dépendances informatiques complexes.

Le problème : L'établissement académique devait analyser l'ensemble des 575 000 documents divulgués afin d'évaluer les risques réglementaires. Des avis juridiques étaient nécessaires dans 40 juridictions, ce qui a fortement accru la complexité et la pression pour satisfaire aux exigences de conformité internationales.

La solution : Chubb a mobilisé des experts juridiques et forensiques, et des techniques avancées de data mining ont repéré les contenus à haut risque, permettant une revue rapide, en grande partie automatisée. Une coordination juridique intercontinentale a garanti des notifications réglementaires précises et transmises dans les délais.

14,2M$

Résultat : La perte s'est élevée à 14,2 millions de dollars, incluant les frais de réponse à l'incident cyber et les pertes liées à l'interruption d'activité. Grâce à une intervention rapide et à un accompagnement juridique coordonné, l'institution académique a évité amendes, enquêtes réglementaires ou sanctions. Malgré l'ampleur de la fuite, les impacts sur la réputation et la conformité ont été efficacement contenus.

Section 10

Événements à grande échelle : les effets d'onde de l'interdépendance

Aucune entreprise ne fonctionne en vase clos : elle dépend de partenaires, de fournisseurs et de clients. Deux cyberattaques marquantes survenues en 2025 montrent à quel point les dommages causés par un ransomware peuvent toucher de nombreuses entreprises, tout au long de la chaîne d'approvisionnement. Si Chubb tirait déjà la sonnette d'alarme sur ce sujet en 2022, la gravité de ces événements apparaît désormais plus clairement dans l'ensemble de l'écosystème cyber.

Royaume-Uni – août 2025

Constructeur automobile mondial

L'attaque survenue fin août 2025 contre un constructeur automobile mondial constitue l'incident cyber le plus dévastateur de l'histoire britannique. Les détails de cet événement font figure d'avertissement, riche d'enseignements essentiels pour toutes les entreprises.

L'incident

Attribuée aux « Scattered Lapsus Hunters », l'attaque a contraint à désactiver les réseaux informatiques mondiaux afin de contenir la brèche.

L'impact opérationnel

La production a été interrompue pendant cinq semaines sur des sites au Royaume-Uni, en Slovaquie, au Brésil et en Chine. Les systèmes paralysés comprenaient les commandes des lignes de production, les outils de conception CAD/PLM et les plateformes de commande des concessionnaires.

Conséquences en matière de sécurité et de droit :

Les pirates ont exfiltré des données de paie et des dossiers clients concernant près de 7,4 millions de personnes, entraînant une vague de procédures judiciaires.

Les répercussions financières systémiques

1,9Md£

Économie

L'économie britannique a subi une perte estimée à £1.9 milliard ($2.5 billion), contribuant au ralentissement du PIB au T3 2025.

1,2Md£

Impact sur la chaîne d'approvisionnement

Plus de 5 000 organisations au Royaume-Uni ont été touchées ; le gouvernement est intervenu avec 1,2 milliard £ de prêts d'urgence pour stabiliser la chaîne.

485M£

Pertes de l'entreprise

Le constructeur automobile mondial a déclaré une perte avant impôts de 485 millions £, effaçant un bénéfice de 398 millions £ réalisé l'année précédente.

États-Unis – février 2025

Violation de données chez Oracle Health

Début 2025, Oracle Health (anciennement Cerner) a été victime d'une violation majeure de données, que des analystes considèrent comme l'une des plus importantes de l'histoire du secteur de la santé aux États-Unis.

L'incident

Des attaquants ont utilisé des identifiants volés pour accéder à d'anciens serveurs de migration de données Cerner, pas encore transférés vers Oracle Cloud.

La vulnérabilité principale

La fuite a visé un environnement ancien, dont certaines parties n'avaient plus été utilisées depuis 2017, montrant que les données « oubliées » constituent une cible de choix.

Les conséquences

L'attaque a dérobé des dossiers provenant d'environ 80 hôpitaux, exposant les numéros de sécurité sociale des patients ainsi que leurs antécédents médicaux, notamment des diagnostics et des images de traitement.

La dimension d'extorsion

Un acteur malveillant, opérant sous le pseudonyme Andrew, a exigé des millions en cryptomonnaie afin d'empêcher la divulgation des fichiers dérobés.

Ces événements et d'autres survenus en 2025 – dont beaucoup résultant d'erreurs ou d'incidents plutôt que d'actes malveillants (p. ex., la panne d'Amazon Web Services en octobre) – rappellent l'urgence d'identifier et de déployer les mesures de réduction des cyberrisques les plus strictes disponibles.

Incident chez un fournisseur (PME)

L'événement : Le détaillant assuré avait fait appel à un prestataire technologique tiers pour le logiciel indispensable à ses opérations quotidiennes. Lorsque ce prestataire a été visé par une attaque par rançongiciel, l'ensemble de ses systèmes est tombé hors ligne.

L'impact : Faute d'accès au logiciel, l'assuré n'a pas pu vendre certains produits, commander du stock ni planifier les rendez-vous clients.

La solution : Chubb a fait appel à un expert-comptable judiciaire afin d'aider l'assuré à chiffrer la perte d'exploitation contingente qui en a résulté. La préparation de l'assuré, grâce à son plan de réponse aux incidents, ainsi que son intégration au dispositif de gestion des sinistres de Chubb, ont permis de mieux gérer un événement largement hors de son contrôle.

1,2M$

Résultat : La perte totale s'est élevée à $1,2 million.

Même si ces scénarios peuvent sembler éloignés des petites entreprises, l'expérience de Chubb montre qu'ils sont bien plus proches de la réalité qu'on ne le pense.

Section 11

Chubb : donner aux entreprises les clés pour réduire le risque cyber grâce à des éclairages

Au-delà des outils de réduction des risques, la connaissance est l'une des meilleures protections face à des cybermenaces en constante évolution. Chubb met à la disposition de ses assurés un ensemble d'analyses et d'informations pour aider à prévenir les incidents cyber et à en limiter l'impact.

L'Index Cyber de Chubb

L'Index Cyber de Chubb, lancé en 2015, offre un accès en temps réel aux données mondiales propriétaires de Chubb sur les sinistres, ainsi qu'à des analyses sur les menaces cyber actuelles, les tendances et les coûts.

La plateforme de recherche permet aux utilisateurs de définir des paramètres et de consulter les tendances historiques selon :

Activité des incidents : Analyse des tendances des cybermenaces qui touchent les organisations — selon la taille, le secteur d'activité et la région géographique.

Coûts des sinistres : Analyse des coûts des sinistres cyber Chubb selon la taille de l'organisation et le secteur d'activité.

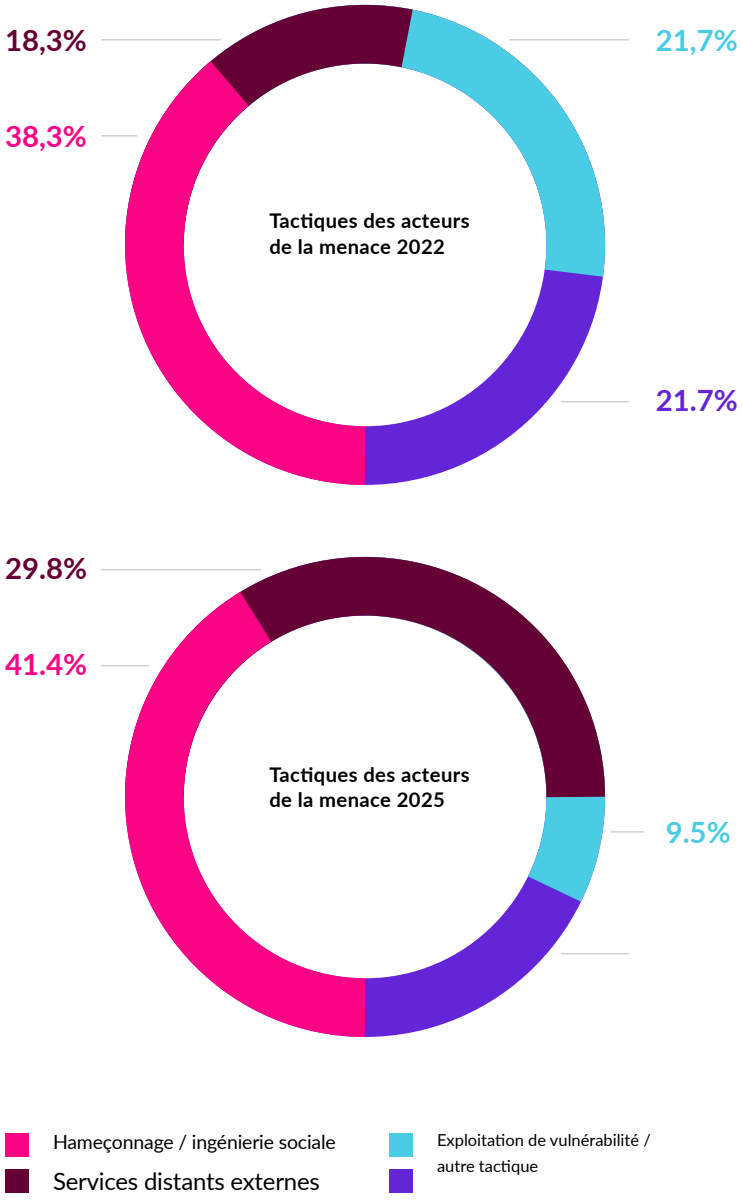
Calculateur de risque cyber: Un outil qui offre une meilleure visibilité sur l'éventail plus large des expositions cyber et sur les coûts potentiels des pertes liées au cyber.

Analyses des achats des pairs : Permet aux entreprises de comparer leur propre protection cyber à celle d'organisations similaires.

Renseignement sur les menaces – Chubb

En complément de notre Rapport sur les sinistres cyber, Chubb publie un rapport trimestriel de Threat Intelligence (renseignement sur les menaces) afin d'offrir aux professionnels de la cybersécurité des éclairages clairs et concrets sur les dernières évolutions des menaces cyber et sur l'expérience de Chubb en matière de sinistres.

Un rapport récent a montré qu'en 2025, la tactique d'accès initial la plus fréquente à l'origine d'un incident de rançongiciel était le phishing. L'exploitation de services distants exposés (p. ex. abus de VPN, ports ouverts) arrivait en deuxième position, tandis que l'exploitation de vulnérabilités critiques se classait troisième.



Par rapport à 2022, la part des sinistres liés à l'exploitation de vulnérabilités critiques est passée de près de 22 % à 9 % – en cohérence avec le lancement par Chubb de son programme de sensibilisation à la gestion des vulnérabilités, dans le cadre duquel notre équipe de Cyber Threat Intelligence donne la priorité aux vulnérabilités exploitables les plus critiques et envoie des alertes ciblées uniquement aux assurés susceptibles d'être concernés. L'équipe Threat Intelligence de Chubb se concentre exclusivement sur les vulnérabilités exploitables les plus critiques et adresse des alertes ciblées uniquement aux assurés susceptibles d'être concernés. Ce service est proposé gratuitement à tous les assurés Chubb Cyber.

Grâce à notre programme de sensibilisation à la gestion des vulnérabilités (Vulnerability Management Outreach Program), Chubb analyse en continu son portefeuille et informe les courtiers et les assurés des failles graves et exploitables nécessitant l'application de correctifs, que ce soit au renouvellement ou pendant la période de couverture. Ce service est proposé à titre gratuit à l'ensemble des assurés Chubb Cyber.

En complément de notre Vulnerability Management Outreach Program, Chubb propose des services axés sur le phishing afin d'aider les assurés à réduire leur exposition aux attaques d'hameçonnage, notamment :

Formation

Modules et jeux de sensibilisation à la sécurité et de prévention du phishing pour les employés, basés sur les menaces les plus récentes.

Tests

Simulations d'e-mails de phishing, y compris des simulations reposant sur la technologie deepfake, pour évaluer la prise de décision des employés.

Technologie

Un outil de sécurité e-mail, dopé à l'IA, pour aider à repérer l'intention de phishing, les anomalies de langage et de comportement qu'un humain risque de ne pas voir.

Section 12

Conclusion

Résilience à l'ère de l'accélération

En 2025, le risque cyber a été marqué par une accélération. Des attaques d'IA autonomes, l'élargissement des réglementations sur la vie privée et des stratégies d'arbitrage de masse font partie des facteurs qui raccourcissent les délais et amplifient les conséquences potentielles des incidents cyber.

Investir dans des capacités de détection avancées, renforcer la gouvernance des pratiques liées à l'IA et aux données, et mettre à l'épreuve les écosystèmes de tiers figurent parmi les nombreux leviers permettant aux organisations de réduire concrètement leur vulnérabilité.

Comme depuis des décennies, Chubb est là pour vous accompagner. Notre expérience cyber à l'échelle mondiale, la richesse de nos données de sinistres et nos capacités intégrées de prévention des risques et de réponse donnent à nos clients les moyens d'anticiper, de résister et de se remettre des cyberévénements complexes d'aujourd'hui – et de se préparer à la suite. Nous avons hâte de poursuivre notre collaboration avec des clients partout dans le monde, en renforçant leur résilience financière et opérationnelle face au risque cyber.

Pour en savoir plus, rendez-vous sur

Assurance cyber Chubb

CHUBB®

Comptez sur Chubb pour une protection cyber complète et une résilience renforcée.