Risques cyber systémiques :

FAQ courtiers

CHUBB®

Chubb s'est engagé à rester un leader de l'assurance cyber en innovant, orientant et structurant son approche afin d'assurer sa pérennité sur le secteur.

Aujourd'hui, la fréquence et la sévérité des incidents cyber incitent les assureurs à revoir leur tarification et plus généralement leurs termes et conditions. Ces derniers mois, de multiples événements cyber de grande ampleur ont compromis des cibles allant de fournisseurs de solutions logicielles et fournisseurs de sécurité des messages électroniques aux infrastructures et serveurs de données. Ces événements ont impliqué plusieurs types de cyberattaques susceptibles de dégénérer en événements de grandes ampleurs.

En conséquence, Chubb développe des solutions innovantes visant à gérer ces risques. Chubb continuera à offrir les couvertures cyber standardsque ses assurés et ses partenaires de distribution connaissent bien. Cependant, nous restructurons également notre approche concernant les événements systémiques et collaborons avec les acteurs du secteur et les gouvernements afin de trouver plusieurs moyens de délivrer des garanties claires et précises pour toutes les parties.

Impact sur les courtiers et les assurés cyber

Chubb prévoit que nos nouvelles solutions apporteront à nos partenaires une meilleure stabilité et un développement à long terme sur le marché de l'assurance cyber. Les courtiers auront une belle opportunité de démontrer leur expertise aux clients, notamment en illustrant clairement l'importance de l'assurance en cas de risques systémiques, en personnalisant les garanties pour couvrir les risques spécifiques de leur client, et en complétant l'offre avec des services prévention et de conseil à forte valeur ajoutée . La nouvelle approche de Chubb s'appuiera sur des concepts familiers pour la plupart des courtiers et des clients qui ont l'expérience de l'assurance de dommages aux biens et des catastrophes naturelles. A terme, une approche structurée pour quantifier le risque cyber catastrophique devrait se traduire par une augmentation de la capacité sur le marché.

FAQ marché/ risque cyber

Quelles sont les motivations à l'origine des changements de stratégie actuels en matière d'assurance cyber ?

Les incidents cyber et les menaces sont en augmentation et évoluent. Plus de 18 000 nouvelles vulnérabilités logicielles ont été publiées en 2020, soit près de trois fois plus qu'en 2015, et celles-ci sont en croissance constante. Parallèlement, près de 1,2 million nouveaux logiciels malveillants ont été identifiées en 2020, soit plus du double par rapport à 2015. Alors que certaines typologies d'attaques comme les rançongiciels sont devenues plus courantes et plus coûteuses, la compromission des e-mails professionnels et les violations de données continuent de faire grimper la fréquence des incidents cyber à des niveaux parmi les plus élevés jamais atteints, facilitée notamment par l'augmentation du travail à distance. La fréquence et la sévérité croissantes de ces incidents cyber pèsent sur les ratios sinistres à prime des assureurs, tandis que les risques systémiques à potentiel catastrophique sont de plus en plus manifestes.

D'autres organisations partagent-elles le point de vue de Chubb sur le sujet du risque cyber systémique ?

Oui, nous pensons que d'autres organisations, gouvernements, régulateurs, et agences de notation ont également constaté l'ampleur et l'urgence de ce sujet. En 2020, le Congrès américain a formé la Cyberspace Solarium Commission, présidée par le sénateur Angus King (I-ME) et le représentant Mike Gallagher (R-WI). Après une étude d'un an, la Commission a conclu que les États-Unis risquent de subir une cyberattaque catastrophique et qu'ils sont "en danger d'insécurité dans le cyberespace". En Europe, l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) a été créée il y a plus de 15 ans pour faire face au nombre croissant de d'incidents cyber graves touchant les secteurs publics et privés.

Son rapport, publié en avril 2021, souligne qu'à la lumière des menaces actuelles qui pèsent sur la cybersécurité, la main-d'œuvre mondiale en cybersécurité devrait augmenter de 89 % pour que les organisations puissent défendre efficacement leur actifs en matière de technologies de l'information et de la communication (ICT).Afin de faire face à cette situation critique, les gouvernements nationaux ont commencé à mettre en œuvre un certain nombre de programmes et de politiques.

En France, le Président de la République, Emmanuel Macron, a inauguré en février 2022 un Campus Cyber qui prévoit de mettre en place des actions visant à fédérer la communauté de la cybersécurité et à développer des synergies entre ces différents acteurs.

En outre, l'agence de notation AM Best a indiqué en juin 2021 que "les perspectives du marché de l'assurance cyber sont sombres", mentionnant "les implications profondes des effets en cascade des risques cyber et l'absence de frontières géographiques ou commerciales ». Elle a conclu que les assureurs "dont la gestion des risques est déficiente en matière de cyber peuvent être soumis à un risque d'accumulation dépassant leur tolérance au risque et subir une pression sur leur notation".

Veuillez consulter les liens ci-dessous pour accéder aux observations d'autres organisations :

- Executive Order on Improving the Nation's Cybersecurity (US Government): www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
- Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market (US Government Accountability Office): www.gao.gov/products/gao-21-477
- Cyber Insurance Rates Could Rise 50% in 2021 (MarshMcLennan Agency): www.marshmma.com/blog/cyber-insurance-rates-could-rise-50-in-2021
- Balancing Risk and Opportunity Through Better Decisions (Aon): www.aon.com/2021-cyber-security-risk-report/

Comment la stratégie de Chubb se positionne-t-elle au sein du secteur ?

La plupart des acteurs en assurance cyber se concentrent sur la problématique particulière des rançongiciels et de l'adéquation des tarifs en réduisant les capacités, en augmentant les tarifs et en procédant à des ajustements spécifiques en fonction du secteur ou de l'exposition. Alors que Chubb met en place des mesures similaires, le groupe s'appuie également sur des dizaines d'années d'expérience et sur son envergure commerciale bien plus grande pour se concentrer sur un problème plus vaste : la gestion des risques cyber systémiques. Bien que d'autres organisations aient évoqué la nécessité d'une telle gestion dans le secteur, peu de mesures concrètes ont été prises jusqu'à présent. Il est probable que Chubb prenne la tête du mouvement dans ce domaine.

Est-ce que des techniques de souscription avancées des risques cyber peut atténuer le risque de catastrophes cyber ?

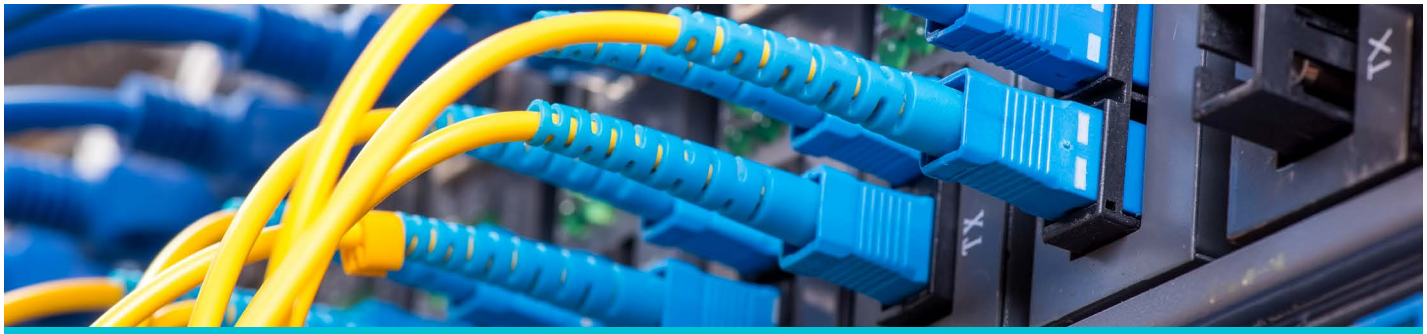
Chubb dispose d'une équipe d'ingénieurs et de souscripteurs spécialisés dans les risques cyber. Nous introduisons de nouveaux outils d'analyse des menaces et de l'Intelligence Artificielle dans nos processus de souscription. De plus, nous offrons à nos assurés l'accès à une gamme complète de services de prévention et d'atténuation des risques. Grâce à notre proactivité dans ces domaines, les résultats de souscription de Chubb en matière d'assurance cyber dépassent ceux de l'ensemble du secteur. Mais malgré ces investissements importants, de nombreuses menaces cyber sont conçues spécifiquement pour échapper aux contrôles internes et aux meilleures pratiques. Aucun contrôle de souscription ou de prévention ne peut éliminer complètement le risque de catastrophes cyber.

Qu'est-ce qu'un risque cyber systémique ? Comment Chubb définit-il ce terme ?

Selon nous, le terme « systémique » fait référence à un risque qui a le potentiel d'infliger des dommages étendus en raison de points communs ou d'éléments partagés en matière de risque, tandis que le terme « catastrophique » désigne un risque systémique qui se manifeste par des pertes sévères ou importantes pour de nombreux assurés.

Quels risques cyber catastrophiques ont émergé ces dernières années ?

La dépendance toujours plus grande des organisations et des consommateurs à l'égard de la technologie, ainsi que l'interconnectivité des technologies et des partenaires, ont créé un environnement dans lequel les risques cyber peuvent se développer de manière exponentielle. Les incidents cyber ont également un impact plus étendu. Sur une période de 100 jours, entre décembre 2020 et mars 2021, plusieurs attaques majeures ont compromis des cibles allant de fournisseurs de solutions logicielles et fournisseurs de sécurité des messages électroniques aux Datacentres et aux infrastructures publiques. Au total, plus de 100 000 organisations dans le monde ont été touchées par ces événements, entraînant des perturbations pour des millions de clients et de citoyens, ainsi que des pertes économiques. A titre d'exemple, l'attaque connue sous le nom de Solorigate, où un code malveillant était intégré dans une mise à jour d'un logiciel d'analyse de réseau, a affecté 20 000 entreprises et agences gouvernementales. Les conséquences auraient pu être bien plus graves si l'intention avait été de dérober ou de détruire des données critiques ou d'autres informations.



Les types de risques suivants, en particulier lorsqu'ils sont combinés, ont été identifiés comme ayant le potentiel de dégénérer en événements catastrophiques :

Les événements exploitant des vulnérabilités connues critiques :
Certaines vulnérabilités logicielles connues n'ayant pas fait l'objet de correctif peuvent être sévères et donc faciles à exploiter. Elles peuvent être déployées à distance avec des privilèges d'accès limités et avoir un impact négatif significatif.[6]

Les vulnérabilités « zero-day » :
Certaines vulnérabilités logicielles, connues des cybercriminels mais pas encore de tous, peuvent être facilement exploitables. Elles sont potentiellement sévères et ne bénéficient souvent d'aucune protection.

Les événements visant la chaîne d'approvisionnement logiciel (Vulnérabilités Fournisseur):
Ces attaques sont en fait un cheval de Troie permettant aux pirates de pénétrer dans les systèmes par le biais de logiciels fiables et certifiés.

Les pannes d'infrastructures :
Les infrastructures critiques, comme les réseaux électriques et les services de télécommunications, sont confrontées à un risque potentiel de défaillance à très grande échelle, que ce soit à la suite d'une attaque cyber ou d'incidents cyber non malveillants, notamment des défaillances de systèmes, des erreurs humaines ou des erreurs de programmation. La récente attaque contre Colonial Pipeline, la société d'approvisionnement en carburant desservant la côte Est des États-Unis, a généré une indisponibilité de l'infrastructure suite à une attaque par rançongiciel, ayant provoqué des pénuries de carburant pour des millions de citoyens et d'entreprises dans plusieurs États.

Les autres événements systémiques :
Certains types de cyberattaques peuvent être menés simultanément ou automatiquement contre un grand nombre de victimes, provoquant finalement un événement cyber catastrophique. Internet et certains services de télécommunications ont atteint un niveau d'infrastructure sociétale critique, et certaines grandes entreprises du cloud sont si largement utilisées qu'une panne généralisée aurait des répercussions sur les activités de milliers voire de millions d'entreprises.

Les événements de type rançongiciel :
Bien qu'elles ne soient pas nécessairement systémiques par nature, les attaques par rançongiciel, qui prennent en otage les fichiers électroniques ou les informations des organisations ou des personnes ciblées jusqu'au versement d'une rançon, sont désormais menées avec une efficacité industrielle. Certaines attaques destructrices peuvent se faire passer pour des rançongiciels, comme les événements NotPetya et WannaCry.

Nous parlons des rançongiciels depuis des années. Est-ce que Chubb les considère différemment aujourd'hui ?

Nous analysons les tendances en matière de rançongiciel depuis plusieurs années et nos stratégies de souscription se sont adaptées au gré de leur évolution. Afin d'aider à gérer ces risques, nous avons réagi en modifiant la stratégie de souscription (par exemple, en évitant certaines typologies ou catégories d'entreprises qui ne disposent pas de certaines mesures de sécurité), les franchises, les limites et la co-assurance. Chubb s'appuie également sur une souscription dite « signal-based » qui analyse les facteurs et les signaux de risque obtenus de diverses sources internes et externes pour nous aider à identifier les risques pour les clients et les prospects.

Le nouveau produit cyber offrira encore plus de possibilités d'adapter le niveau des sous-limites, de la co-assurance et des franchises pour les rançongiciels concernant différentes garanties.

Combien de sinistres liés au risque cyber systémique Chubb a-t-il reçu jusqu'à présent ?

Chubb a reçu des centaines de notifications liées aux principaux incidents cyber systémiques survenus au cours des neuf derniers mois.

Pourquoi continuons-nous à voir tant de changements sur le marché cyber ? Le secteur de l'assurance a-t-il connu des bouleversements similaires dans d'autres lignes d'activité ?

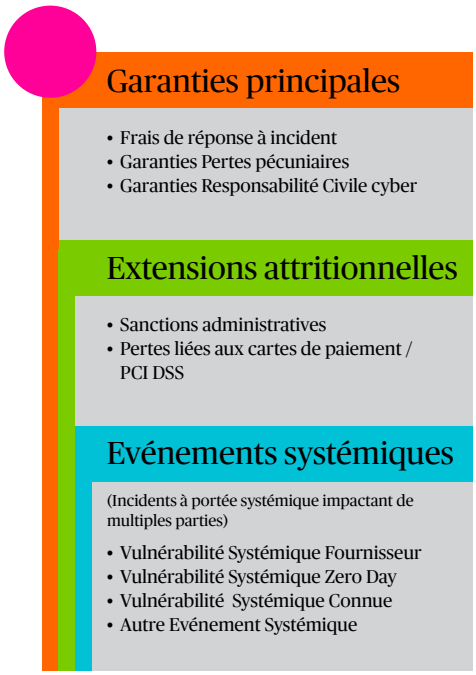
L'assurance cyber n'a atteint sa maturité qu'au cours des dernières années et reste une ligne en pleine évolution. Dans le même temps, les risques contre lesquels elle protège sont dynamiques et caractérisés par une complexité et une gravité qui s'accentue rapidement. Historiquement, le marché de l'assurance de dommages aux biens a subi des chocs d'événements soudains et d'une ampleur sans précédent, notamment le tremblement de terre de San Francisco de 1906 et les attentats terroristes du 11 septembre. Les solutions apportées après coup ont permis de clarifier les risques concernés et de proposer des couvertures distinctes pour les risques catastrophiques. En matière d'assurance cyber, nous avons l'occasion d'agir sur la conception des produits et de créer éventuellement des solutions avec les gouvernements avant la survenue du fait, ce qui peut apporter une stabilité au marché de l'assurance et une garantie de couverture pour les clients.

Offre de produit cyber Chubb

Est-ce que Chubb continuera d'offrir les mêmes couvertures cyber que celles qu'elle propose actuellement ?

Les couvertures standards que nous offrons aujourd'hui - frais de réponse à incident, dommages immatériels, responsabilité civile cyber - continueront d'être disponibles. En outre, Chubb fait une distinction entre les événements circonscrits et les événements systémiques. Nous estimons que le cœur de nos produits permettra de couvrir environ 90 % des incidents dans le cadre des couvertures standards pour les événements circonscrits.

Chubb souscrira les risques attritionnels importants, mais proposera également des couvertures supplémentaires pour les risques systémiques potentiellement généralisés et catastrophiques sous forme d'extensions du produit principal cyber, permettant ainsi de de proposer des garanties d'une manière plus structurée et durable. Ces couvertures seront désignées collectivement sous le terme de couvertures d'« événements systémiques » et incluront différentes sous-composantes décrites dans la police d'assurance. Les événements systémiques et chaque sous-composant seront soumis à des limites, franchises, et montant de co-assurance spécifiques. Cette approche est similaire à celle de l'assurance dommages aux biens et de son traitement des risques catastrophiques, tels que les inondations et les tremblements de terre, depuis plus d'un siècle.



Process de souscription

Quels types d'extensions de couverture devons-nous prévoir ?

Chubb offrira des extensions de couverture distinctes pour tenir compte des événements systémiques, comme les failles de la chaîne d'approvisionnement, les atteintes graves de type « zero-day » et les exploitations graves de vulnérabilité.

Le schéma sur la gauche donne une vision globale de la répartition des garanties.

Les clients et les prospects devront travailler avec leur courtier pour déterminer les risques cyber auxquels ils peuvent être confrontés du fait de leurs opérations et de leur environnement informatique, puis sélectionner les extensions de couverture qui leur conviennent le mieux.

Est-ce que Chubb va changer sa tarification des couvertures cyber ?

La tarification continuera de refléter les besoins spécifiques d'assurance et le profil de risque de chaque client.

Quand ces changements de produits entreront-ils en vigueur ?

Chubb va utiliser cette nouvelle approche sur l'ensemble des segments dans les mois à venir. Il est essentiel de commencer à travailler avec les risk managers très en amont des renouvellements afin d'identifier leurs risques spécifiques et de déterminer quelles extensions de couverture leur fourniront le bon niveau de protection.

Y aura-t-il un document commercial que nous pourrons joindre au formulaire pour en expliquer les avantages ?

Oui, une synthèse du produit est disponible. Vous pouvez la télécharger ici.

Que faire pour se préparer à ces changements? Des ressources me seront-elles fournies pour guider mes discussions avec les clients et les prospects?

Outre la lecture et la compréhension de ces FAQ, nous vous recommandons de profiter de toutes les formations et les webinaires qui vous seront proposés par Chubb. Des ressources telles que des rapports, des webinaires et des vidéos seront mis à votre disposition tout au long de l'année. Vous pourrez les partager avec vos clients assurés. Vous pouvez également vous rendre sur le site internet Chubb ou contacter vos souscripteurs cyber pour plus d'informations.

Process de cotation

Y a-t-il des éléments qui guideront la souscription et la tarification des couvertures des événements systémiques ?

Oui, plusieurs facteurs détermineront la couverture d'événements systémiques et la tarification proposées par Chubb, notamment les dépendances critiques de l'organisation, les engagements contractuels avec les fournisseurs de services, l'hygiène et les contrôles en matière de cybersécurité, ainsi que le plan et les tests de réponse à incident.

Qu'est-ce qui change dans la structure tarifaire de la couverture des événements systémiques ?

Chubb s'engage à la plus grande transparence vis-à-vis de ses clients et proposera pour la couverture des événements systémiques un tarification distincte, avec des options de limites et de franchises.

Formulaire de police

Quelle couverture est exclue dans les nouveaux produits cyber de Chubb ?

La couverture des événements systémiques n'est pas exclue. Elle est structurée pour fournir de manière transparente une capacité pour les événements souscrits. Les assurés ont la possibilité d'acheter une couverture pour les événements systémiques, mais ce n'est pas obligatoire.

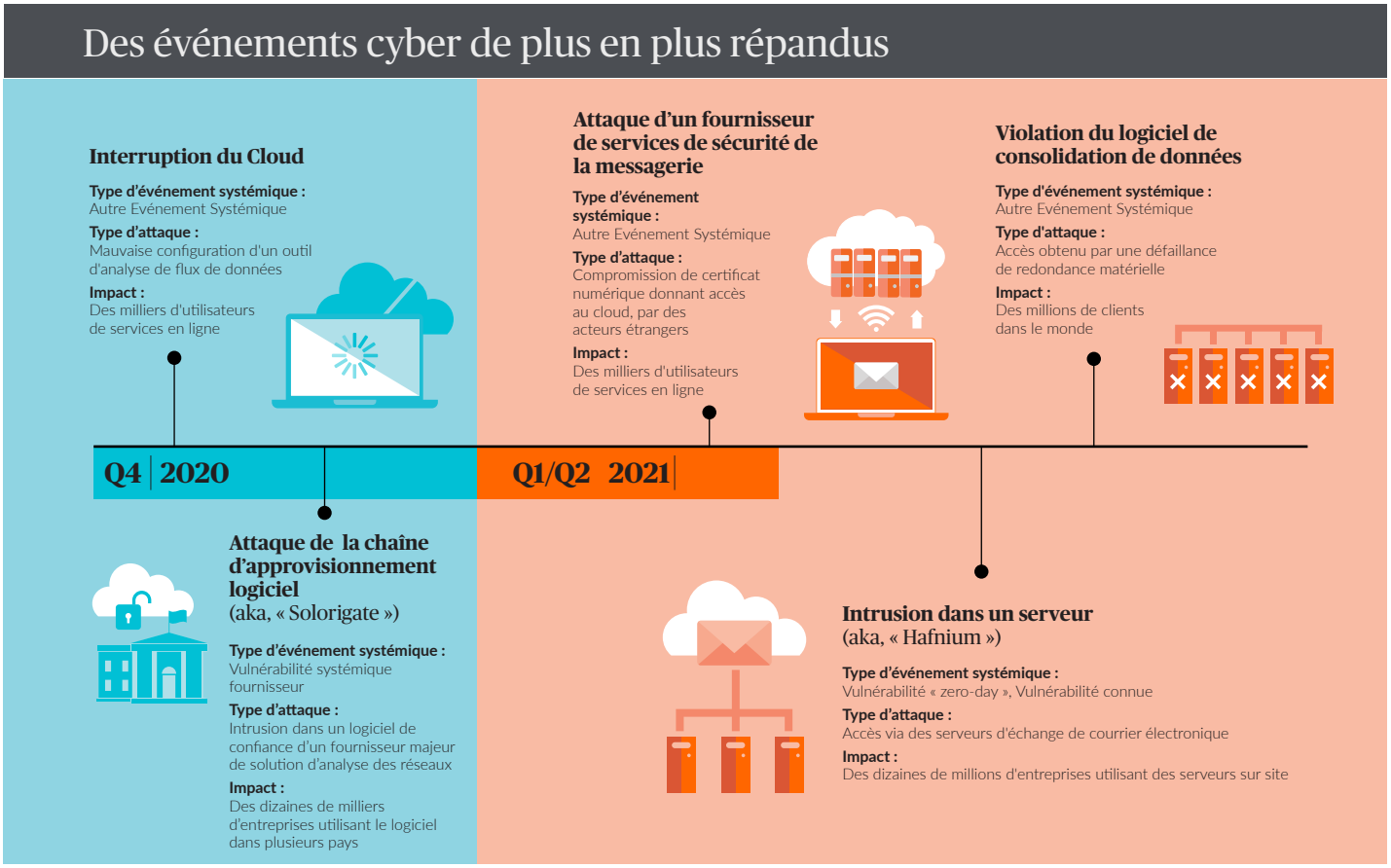
Où sont décrits les concepts d'événements circonscrits et d'événements systémiques dans la police d'assurance ?

La première page de l'avenant présent au sein la police stipule que les incidents cyber seront classés dans les catégories suivantes : Evénements Circonscrits ou Evénements Systémiques. Les définitions sont également présentées dans l'avenant dédié présent au sein de la police. Les autres définitions clés utilisées dans le cadre de ces concepts sont notamment les suivantes : Origine Systémique et Groupe d'Impact Restreint, entre autres.

Pour les polices qui prévoient les mêmes limites, franchises et co-assurances pour tous les types d'événements systémiques, il n'est pas important de différencier les quatre sous-catégories d'événements systémiques. Cependant, s'il existe des limites, des franchises ou des co-assurances différentes, alors les définitions suivantes des sous-catégories d'événements systémiques doivent être examinées :

- Vulnérabilités Systémiques Connues
- Vulnérabilités Systémiques Nouvelles
- Vulnérabilité Systémique Fournisseur
- Autres Evénements Systémiques

Les modifications de l'avenant concernant la section 7.1 (Conditions Générales communes) de la police traite des "Obligations en cas d'incident cyber" et décrit en détail la façon dont le titulaire de la police et Chubb collaboreront en cas d'incident cyber. Cette section comprend des informations sur le calendrier et les méthodes permettant de déterminer si un incident cyber est un événement circonscrit ou un événement systémique. Comme toujours, le texte de police doit être lu dans son intégralité.



Pouvez-vous fournir des exemples réels d'événements systémiques ?

Des exemples récents d'événements systémiques sont décrits dans l'infographie ci-dessus.

Comment fonctionne la co-assurance ? Pouvez-vous donner un exemple ?

La part de co-assurance applicable aux Evénements Systémiques, aux Incidents Rançongiciels et Carence de Mise à Jour est une co-assurance dite de « réduction des pertes » ce qui signifie que la part de co-assurance de l'assuré n'épuise pas les limites de l'assurance. Au contraire, la responsabilité pour chaque sinistre est répartie entre l'assuré et l'assureur, et la part de l'assureur est alors soumise à la limite applicable à ce risque.

Par exemple, si une police comporte une sous-limite de 5 % d'une limite globale de 10 millions d'euros pour un Evénement Systémique, l'engagement maximum de l'assureur pour toute perte liée à un Evénement Systémique en vertu de cette sous-limite d'Evénement Systémique sera de 500 000 € (c'est-à-dire 5 % de 10 millions d'euros).

Si la couverture d'un Evénement Systémique est soumise à une co-assurance de 50 %, une perte de 1 million d'euros sera répartie à parts égales entre l'assuré et l'assureur, et la sous-limite pour Evénement Systémique sera alors épuisée parce que l'assureur aura payé la totalité de la sous-limite disponible de 500 000 €.

Autre cas, si la perte liée à un Evénement Systémique s'élève à 500 000 €, elle sera répartie à parts égales, mais comme l'assureur ne paiera que 250 000 € dans cette situation, il restera 250 000 € dans la sous-limite d'Evénement Systémique pour des sinistres futurs.

Notes de bas de page

1. National Institute of Standards and Technology's National Vulnerability Database. Accessed at https://nvd.nist.gov/vuln/search
2. AV-TEST Institute (2021). Accessed at www.av-test.org/en/statistics/malware/
3. Federal Commission Warns Dangerously Insecure U.S. At Risk of 'Catastrophic' Cyber Attack (2020). Accessed at www.forbes.com/sites/daveywinder/2020/03/14/make-america-safe-again-federal-commission-warns-us-at-risk-of-catastrophic-cyber-attack/?sh=244402e34d27
4. Ransomware and Aggregation Issues Call for New Approaches to Cyber Risk (2021). Accessed at www.insurancejournal.com/research/research/ransomware-and-aggregation-issues-call-for-new-approaches-to-cyber-risk/
5. Ibid.
6. NIST Security Vulnerability Trends in 2020: An Analysis (2021). Accessed at www.redscan.com/media/Redscan_NIST-Vulnerability-Analysis-2020_v1.0.pdf

À propos de Chubb

Chubb est la société d'assurance IARD cotée en bourse la plus importante au monde. Présente dans 54 pays, Chubb offre des assurances de dommages et de responsabilités aux particuliers et aux entreprises, des assurances santé et prévoyance aux particuliers, de la réassurance et des assurances vie à un éventail de clients très diversifié. En tant que compagnie de souscription, Chubb évalue, couvre et gère les risques avec connaissance et discipline. Elle indemnise les sinistres de manière juste et rapide. Chubb se caractérise par l'étendue de son offre de produits et de ses prestations de services, l'ampleur de son réseau de distribution, son exceptionnelle solidité financière, son expertise en matière de souscription, l'excellente qualité de sa gestion de sinistres et de ses activités dans les divers pays du monde. La société mère Chubb Limited est cotée à la bourse de New York (NYSE : CB) et est intégrée à l'indice S&P 500. Chubb dispose de bureaux de direction à Zurich, New York, Londres, Paris et d'autres villes et emploie environ 31 000 personnes à travers le monde. Retrouvez plus d'informations sur www.chubb.com

Pour en savoir plus sur l'expérience et l'expertise de premier plan de Chubb en matière de gestion des risques cyber, rendez-vous sur le site www.chubb.com/fr/cyber

Chubb. Insured.℠

Chubb European Group SE, entreprise régie par le Code des assurances, au capital social de 896 176 662 euros, sise La Tour Carpe Diem, 31 Place des Corolles, Esplanade Nord, 92400 Courbevoie, immatriculée au RCS de Nanterre sous le numéro 450 327 374. Chubb European Group SE est soumise au contrôle de l'Autorité de Contrôle Prudentiel et de Résolution (ACPR) située 4, Place de Budapest, CS 92459,75436 PARIS CEDEX 09.