Les risques cyber catastrophiques

Une préoccupation grandissante

CHUBB

Les incidents cyber peuvent engendrer des pertes qui ne sont limitées ni par le temps, ni par la géographie.

Avec la digitalisation du monde, la fréquence, la gravité et la sophistication des incidents cyber sont en augmentation, de même que la dépendance à la technologie. Les vulnérabilités et les expositions se multiplient en raison d'une plus grande interconnexion, créant des risques systémiques de grande ampleur, croissants et difficiles à détecter ou à contrôler. La combinaison de ces risques systémiques avec des conséquences potentiellement graves et étendues rend possible la survenance d'une catastrophe cyber.

À l'instar des pandémies, les incidents cyber peuvent engendrer des pertes qui ne sont limitées ni par le temps, ni par la géographie. Ce n'est plus une théorie: les cybercriminels ont déjà démontré leur capacité à perturber les chaînes d'approvisionnement d'entreprises du monde entier et à paralyser des infrastructures critiques, comme dans le cas de la récente attaque qui a entraîné la fermeture par Colonial Pipeline de ses lignes d'approvisionnement en carburant de la côte est des États-Unis. Les récents incidents cyber ayant entraîné des milliards de dollars de pertes économiques, il n'est pas difficile d'imaginer une attaque catastrophique qui pourrait mettre à l'épreuve les capacités financières du secteur des assurances.

Contrairement aux précédents événements catastrophiques, nous assistons à une escalade continue des risques cyber. Cet avertissement est l'occasion de mettre en place des défenses contre les risques cyber et des garanties économiques avant qu'une catastrophe ne se produise.

L'assurance cyber arrive à maturité

L'adoption croissante des solutions d'assurance cyber signifie que davantage d'entreprises sont protégées, mais également que l'agrégation des risques cyber se développe pour le secteur de l'assurance.

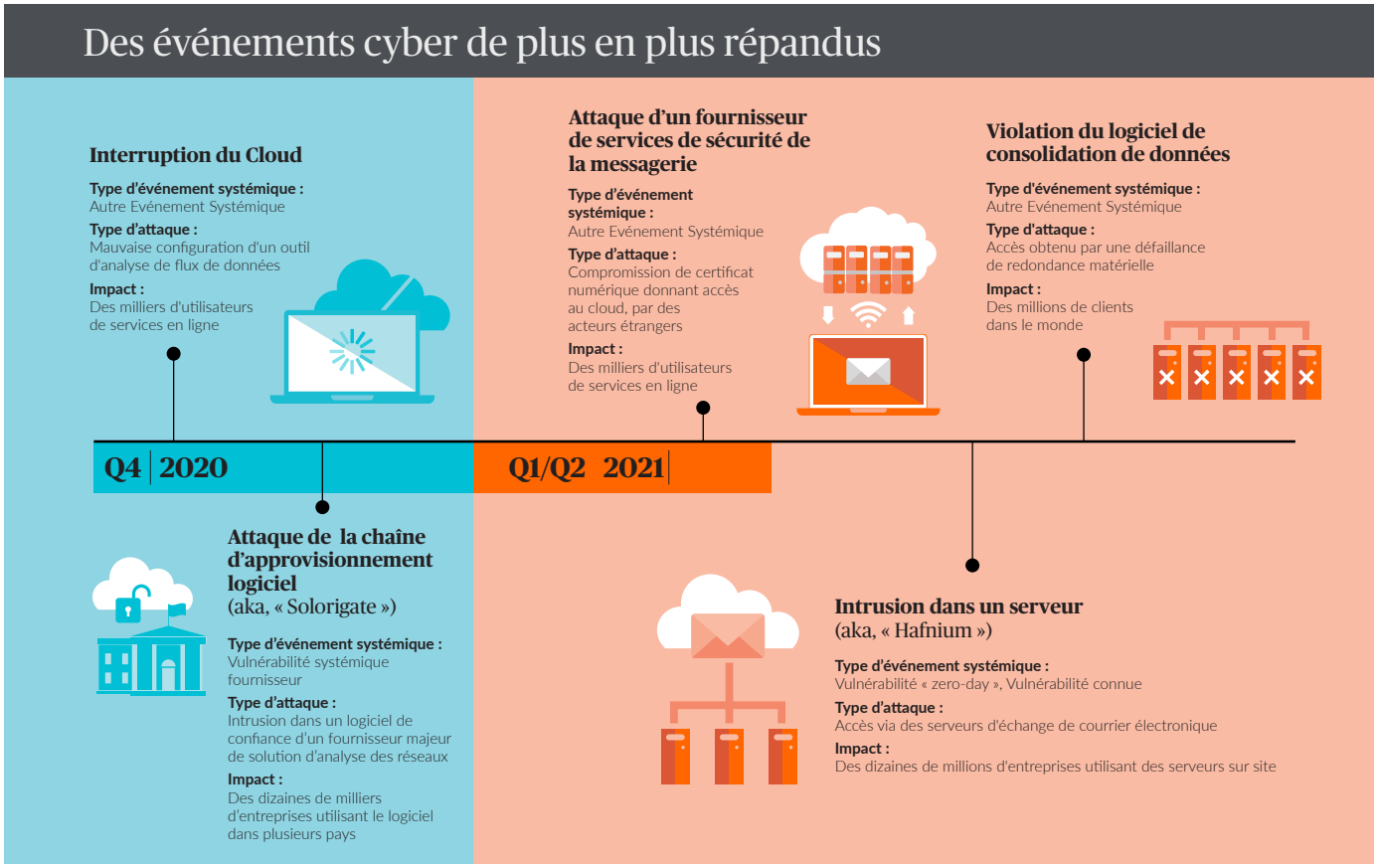
La promesse de l'assurance cyber a été pleinement tenue ces dernières années, les pertes couvertes par les assureurs après des événements cyber significatifs ayant permis de protéger de nombreuses organisations à travers le monde.

Aujourd'hui, les couvertures standards - frais de réponse à incident, dommages immatériels subis, responsabilité civile cyber - offrent des solutions intéressantes de transfert et de gestion des risques aux organisations de toutes tailles et de tous secteurs. De plus, les services d'atténuation des risques cyber proposés par les assureurs ont été très utiles pour aider les entreprises à réduire leurs risques et à améliorer leur sécurité informatique en amont, tandis que les équipes de réponse à incident se sont révélées efficaces pour permettre une reprise d'activité plus rapide suite à un incident cyber.

L'adoption croissante des solutions d'assurance cyber - estimée aujourd'hui à près de 4 millions de polices pour les assureurs Américains et non Américains et à environ 50 % des entreprises américaines couvertes, selon un rapport du Government Accountability Office de mai 2021[1] - signifie que davantage d'entreprises sont protégées, mais également que l'agrégation des risques cyber se développe pour le secteur de l'assurance.

Dans le même temps, les entreprises ont également amélioré leur cyber-résilience au cours des dernières années. En 2020, 53 % des professionnels de l'informatique et de la sécurité informatique interrogés dans le monde entier ont déclaré que leur organisation avait atteint un niveau élevé de cyber-résilience, contre 35 % en 2015.[2]

Si l'assurance cyber joue clairement un rôle de plus en plus important dans la gestion du risque cyber des organisations, la capacité des assureurs à absorber le potentiel de perte totale sur le long terme est moins certaine.



Escalade des risques et des impacts

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 infrastructures publiques.

Bien que les organisations soient plus conscientes des risques cyber et de leurs conséquences, les incidents et menaces cyber n'ont de cesse de s'intensifier et d'évoluer.

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 de nouveaux logiciels malveillants ont été identifiées en 2020, soit plus du double par rapport à 2015. Parmi les failles de sécurité s'étant révélées efficaces en 2020, 85 % impliquaient une interaction humaine, comme les schémas d'ingénierie sociale.

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, en particulier pendant la pandémie de COVID-19 et le recours massif au télétravail qui en a résulté.

Les incidents cyber ont également une portée plus systémique. 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 infrastructures publiques. Plus de 100 000 organisations dans le monde ont été touchées par ces événements.

Dans le cas de l'un de ces événements, connu sous le nom de Solorigate, il a été révélé qu'une attaque massive sur un fournisseur de solutions logicielles, où un code malveillant était intégré dans une mise à jour d'un logiciel d'analyse de réseau, était passée inaperçue pendant près de huit mois, affectant près de 20 000 entreprises et agences gouvernementales.

Dans un autre cas, un groupe de pirates présumé soutenu par un État et de syndicats criminels, connu sous le nom d'Hafnium, a exploité une vulnérabilité alors inconnue (« zero-day ») dans un logiciel courant, dans le but d'accéder aux serveurs de centaines de milliers d'entreprises.

Des incidents très médiatisés exacerbent les tensions

Quand verrons-nous un véritable événement cyber catastrophique à la fois systémique et destructeur ?

Aussi invasifs et coûteux qu'ont été les événements Solorigate et Hafnium, ceux-ci auraient pu être bien pires. Il semble que le motif principal de chacune de ces attaques était l'espionnage, mais si l'intention avait été de voler ou de détruire des données critiques ou d'autres informations, les conséquences économiques auraient pu être beaucoup plus importantes. Dans son témoignage devant le Senate Intelligence Committee, Kevin Mandia, PDG de la société de cybersécurité FireEye, a indiqué que les acteurs à l'origine de l'attaque Solorigate disposaient des accès et des capacités nécessaires pour créer de fortes perturbations, s'ils l'avaient voulu.

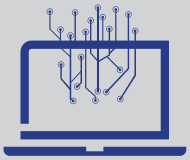
Autre exemple, en 2017, l'attaque NotPetya a exploité un outil logiciel fiscal appelé M.E.Doc utilisé presque exclusivement en Ukraine, mais le logiciel malveillant s'est ensuite propagé sans distinction et a finalement affecté de nombreuses grandes entreprises basées en Europe, aux États-Unis et ailleurs, entraînant des pertes estimées à 10 milliards de dollars. Certaines entreprises victimes de l'attaque NotPetya ont subi des pertes dépassant 100 millions de dollars. Si ce type de logiciel malveillant destructeur avait été déployé lors des attaques de Solorigate ou d'Hafnium, les dommages économiques combinés auraient pu être exponentiellement plus importants que l'événement NotPetya.

La même année, l'attaque par rançongiciel WannaCry a touché plus de 200 000 ordinateurs dans le monde. Heureusement, elle utilisait une vulnérabilité connue pour laquelle un correctif était déjà disponible, de sorte que la plupart des utilisateurs étaient immunisés contre celle-ci. Toutefois, comme dans l'exemple d'Hafnium cité précédemment, l'impact aurait pu être beaucoup plus grave et étendu si le rançongiciel avait exploité une vulnérabilité de type « zero-day ».

À ce jour, nous avons été témoins d'événements systémiques (par exemple Solorigate, Hafnium) et d'autres destructeurs (par exemple NotPetya, WannaCry), mais les sinistres résultant de ces événements ont pu être gérés jusqu'à présent. Avec un tel potentiel de pertes, quand verrons-nous un véritable événement cyber catastrophique à la fois systémique et destructeur ?

Les potentiels événements cyber catastrophiques

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 la gravité des risques cyber peut se développer de manière exponentielle. Les types d'événements suivants, en particulier lorsqu'ils sont combinés, ont été identifiés comme ayant un potentiel catastrophique.



Les événements exploitant des vulnérabilités connues critiques :
En moyenne, environ 50 nouvelles vulnérabilités logicielles sont publiées chaque jour. Sans l'application de correctifs, elles peuvent être exploitées pour des attaques cyber. Environ 15 % d'entre elles sont critiques, ce qui signifie qu'elles sont faciles à exploiter, peuvent être déployées à distance avec des privilèges d'accès limités et ont un impact négatif significatif. Étant donné que les vulnérabilités critiques sont largement connues et qu'elles peuvent être identifiées sur les réseaux des victimes potentielles par des techniques d'analyse Internet courantes, les entreprises ne traitant pas ces vulnérabilités logicielles critiques courent un risque élevé d'attaque.

Les événements vulnérabilité « zero-day » :
Les vulnérabilités logicielles de type « zero-day » sont surtout connues des cybercriminels. Elles sont particulièrement préoccupantes, certaines étant facilement exploitables, potentiellement critiques et souvent dépourvues de protection. En d'autres termes, même les entreprises disposant de programmes bien rodés de gestion des risques cyber peuvent être exposées à des attaques de type « zero-day ».

Les événements visant la chaîne d'approvisionnement logiciel (Vulnérabilités Fournisseur) :
Les attaques visant la chaîne d'approvisionnement logiciel sont en fait un cheval de Troie permettant aux pirates de pénétrer dans les systèmes par le biais de logiciels fiables et certifiés. L'opération Solorigate a démontré le haut degré de sophistication des pirates dans l'exploitation des pratiques courantes de développement logiciel employées dans le secteur technologique. Ces attaques, dont beaucoup semblent être pilotées ou soutenues par des États, devraient se poursuivre et potentiellement s'accélérer. Les tensions géopolitiques, notamment entre l'Occident et ses opposants, devraient continuer d'exacerber la menace de ce type d'événements à l'avenir.

Les pannes d'infrastructures :
Les attaques et autres incidents cyber impliquant des infrastructures peuvent avoir des conséquences de grande ampleur. Par exemple, lors de l'attaque de mai 2021 contre Colonial Pipeline, la société d'approvisionnement en carburant desservant la côte est des États-Unis, des cybercriminels étrangers ont tiré parti d'une panne d'infrastructure en procédant à une attaque par rançongiciel, ce qui en a aggravé l'impact. En conséquence, le pipeline a été fermé durant plusieurs jours, provoquant des pénuries d'essence affectant 45 % de l'approvisionnement en carburant de millions de citoyens et d'entreprises dans plusieurs États américains. Le risque de panne d'infrastructure est un cas particulier dans la mesure où il peut résulter d'une cyberattaque, mais aussi de défaillances d'un système, d'erreurs humaines, d'erreurs de programmation ou d'autres types d'incidents cyber non malveillants.

Les autres événements systémiques :
Certains types de cyberattaques peuvent être menés simultanément ou automatiquement contre un grand nombre de victimes. Internet et certains services de télécommunications ont atteint un niveau d'infrastructure sociétale critique, portant le risque potentiel de défaillance à une échelle considérable. Dans certains cas, une société de télécommunications peut être le seul fournisseur d'une grande ville ou d'une ville de taille moyenne. Dans d'autres cas, certaines grandes entreprises du cloud sont si largement utilisées qu'une panne généralisée affecterait les opérations commerciales de milliers voire de millions d'entreprises différentes simultanément. Toute attaque de ce type capable de se déployer en masse pourrait provoquer un événement cyber catastrophique.

Les événements de type rançongiciel :
Bien qu'elles ne soient pas nécessairement catastrophiques 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. Les demandes habituelles, qui se chiffraient au départ en milliers de dollars, ont maintenant atteint des dizaines de millions, et les criminels ciblent des organisations de toutes tailles.

Renforcer la cyber-résilience

Il est plus que jamais essentiel que les organisations se préparent en vue d'une éventuelle catastrophe cyber.

Avec l'augmentation de l'exposition aux risques cyber, aussi bien par la nature des opérations et des environnements informatiques, par la défaillance d'infrastructures communes ou par l'exploitation de vulnérabilités par des acteurs malveillants, il est plus que jamais essentiel que les organisations se préparent en vue d'une éventuelle catastrophe cyber.

Un bon point de départ consiste à comprendre les expositions spécifiques de chaque organisation, à travers le prisme des potentiels événements cyber catastrophiques décrits dans ce document, puis à engager les ressources nécessaires pour améliorer leurs sécurité cyber et leur résilience. Les prestataires informatiques représentant des risques systémiques importants, les organisations doivent procéder à un contrôle préalable approfondi de ces fournisseurs et s'assurer d'un système de redondance et de résilience autour de ces prestataires, en plus d'examiner les clauses d'indemnisation des contrats, afin d'évaluer comment le risque est transféré.

Elles doivent également tirer pleinement parti de l'expertise de leur courtier ou agent d'assurance et de leur compagnie d'assurance cyber. Bien que les équipes chargées de l'informatique, de la gestion des risques et de la continuité des activités puissent avoir toute confiance dans leurs mesures de protection cyber et leur dispositif de réponse à incident, aucune organisation ne pourra jamais être entièrement protégée contre tous les incidents cyber potentiels - en particulier les catastrophes cyber.

De nombreuses compagnies d'assurance proposent une gamme de services de prévention visant à aider les organisations à améliorer leur sécurité informatique, comprenant des évaluations du plan de réponse à incident, des audits de sécurité, des tests de vulnérabilité du réseau et des simulations d'attaques courantes. Les organisations doivent être préparées à réagir en cas de survenance d'un incident cyber. L'équipe d'experts de réponse à incident de l'assureur peut aider à limiter les dommages causés par de tels événements et à rétablir le fonctionnement complet d'une organisation et cela dans les plus brefs délais. Ces services peuvent faire toute la différence entre survivre à un incident cyber majeur et l'appréhender en toute confiance.

Perfectionner les solutions

L'assurance cyber comme l'assurance dommages aux biens est exposée aux événements catastrophiques.

À l'échelle mondiale, les événements cyber catastrophiques ont le potentiel de paralyser l'activité commerciale et les infrastructures critiques. Comme dans le cas de la pandémie de coronavirus, cela exige que le gouvernement et le secteur privé travaillent ensemble sur des sujets importants, tels que la déclaration et le reporting des incidents cyber afin d'améliorer la cohérence des données et la mise en place de cadres juridiques pour dissuader et punir les cybercriminels.

La croissance de la fréquence et de la gravité des incidents cyber incitent les assureurs à revoir leur tarification et leurs conditions. Pour assurer la stabilité du marché de l'assurance cyber tout en tenant compte de l'ampleur potentielle d'un risque catastrophique, il faudra trouver de nouvelles solutions telles que des partenariats avec le gouvernement et des offres de produits d'assurance pour les particuliers. Pour le secteur de l'assurance, le défi consiste à élaborer des polices qui offrent une certitude en matière de couverture, fournissent une protection significative et aident à la fois les clients et les assureurs à gérer les événements cyber attritionnels et catastrophiques.

Les assureurs ont toujours couvert les dommages en cas de catastrophes naturelles, comme les inondations et les tremblements de terre, dans le cadre d'une couverture distincte, afin d'appliquer un tarif transparent et de surveiller leurs expositions. Ce processus a contribué à maintenir la stabilité globale du marché et la disponibilité de la couverture. Par exemple, de nombreux tremblements de terre, inondations et ouragans majeurs survenus au cours du dernier demi-siècle ont eu un impact significatif sur les résultats dans le secteur de l'assurance de dommages aux biens, mais ont rarement conduit à l'insolvabilité des organismes d'assurance. Ainsi, le secteur de l'assurance est demeuré résilient et stable pour les assurés, même après des événements d'ampleur catastrophique.

L'assurance cyber comme l'assurance dommages aux biens est exposée aux événements catastrophiques, et donc, elle pourrait être amenée à évoluer de la même façon que l'assurance dommages aux biens. Le secteur doit adopter une approche proactive, dans laquelle la couverture des événements catastrophiques est proposée séparément des couvertures principales. La couverture des événements catastrophiques ne serait pas exclue mais plutôt clairement délimitée, en veillant à ce que cette couverture distincte soit tarifée de manière transparente, et soumise à une souscription, des limites de couverture et des franchises appropriées pour les clients. Cette approche permettra au secteur de l'assurance cyber de continuer à fournir des solutions innovantes aux assurés, tout en assurant la viabilité à long terme du marché.

À propos de l'auteur

Michael Kessler est Vice-président du Groupe Chubb et Président de la division Global Cyber Risk Practice de Chubb. À ce titre, il supervise toute l'activité cyber, notamment la stratégie, le développement commercial et des produits, la souscription et les prestations de service, ainsi que les performances globales en termes de bénéfices et de pertes. M. Kessler possède près de 30 ans d'expérience dans le domaine de l'assurance et du conseil actuariel et a précédemment occupé les postes de Directeur de la réassurance de Chubb (2016-2021) et d'Actuaire en chef pour l'activité assurance internationale (2008-2016). M. Kessler est titulaire d'un Bachelor of Arts en mathématiques de l'Université Cornell. Il est membre de l'Académie américaine des actuaires et membre de la Casualty Actuarial Society.

Notes de fin de page

1. Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market (2021). Retrieved from www.gao.gov/products/gao-21-477
2. Cyber Resilient Organization Report (2020). Retrieved from www.ibm.com/security/digital-assets/soar/cyber-resilient-organization-report/#/
3. National Institute of Standards and Technology's National Vulnerability Database. Accessed at https://nvd.nist.gov/vuln/search
4. AV-TEST Institute (2021). Accessed at www.av-test.org/en/statistics/malware/
5. Verizon 2021 Data Breach Investigations Report (2021). Retrieved from https://enterprise.verizon.com/resources/reports/2021/2021-data-breach-investigations-report.pdf
6. U.S. Senate Select Committee on Intelligence (2021). Accessed at www.intelligence.senate.gov/hearings/open-hearing-hearing-hack-us-networks-foreign-adversary
7. NIST Security Vulnerability Trends in 2020: An Analysis (2021). Retrieved from 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.

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.[SM]