LLOYD'S

Rapport Risque Emergent 2017

Technologie

Evaluer les coûts
l'exposition au risque cyber décodée

CYENCE

Avis de non responsabilité du Lloyd’s

Ce rapport a été co-produit par le Lloyd’s et Cyence à titre d’information uniquement. Bien qu’une attention particulière a été apportée à la collecte des données et à la préparation du rapport, le Lloyd’s n’accepte aucune responsabilité quant à l’exactitude de ces données ou à leur exhaustivité et exclut expressément toutes responsabilités ou garanties implicites dans les limites autorisées par la loi.

Le Lloyd’s n’accepte aucune responsabilité ou obligation pour toute perte ou dommage de toute nature causé à toute personne en raison de son action ou de son absence d’action à la suite de, ou en lien avec, toute déclaration, fait, figure ou expression d’opinion ou de croyance contenue dans le présent rapport. Ce rapport ne constitue en aucune façon une consultation juridique ou avis.

A propos du Lloyd’s

Le Lloyd's est le marché mondial d’assurance et de réassurance spécialisées. Soutenu par des capitaux mondiaux diversifiés et d’excellentes notations financières, le Lloyd’s s’appuie sur un réseau international pour développer l’assurance au niveau mondial, en donnant aux entreprises et aux collectivités les clés pour renforcer leur résilience et en favorisant la croissance économique mondiale.Le savoir-faire accumulé au fil des siècles fait du Lloyd’s le pilier et l’avenir du monde de l’assurance. Mené par des assureurs et courtiers expérimentés couvrant plus de 200 territoires, le marché du Lloyd’s propose les assurances essentielles, complexes et critiques qui accompagnent le progrès.

A propos de Cyence

Cyence donne les moyens aux assureurs de comprendre l’impact du risque cyber à partir de données en dollars et de probabilités. L’approche unique de Cyence combine la modélisation économique et la modélisation des risques, la cybersécurité et l’analyse du big data pour créer une plate-forme de modélisation du risque cyber à l’échelle économique. La Plateforme Cyence et ses analyses sont utilisées par les leaders de l’industrie de l’assurance tant pour les aider à comprendre et à gérer le risque cyber que pour créer des produits d’assurance innovants.

Contact

Trevor Maynard
Head of Innovation
trevor.maynard@lloyds.com

Pour toute information sur ce rapport et les études du Lloyd’s sur des sujets innovants, merci de contacter innovation@lloyds.com

A propos des auteurs

Trevor Maynard PhD, MSc, FIA has degrees in pure maths and statistics and is a Fellow of the Institute of Actuaries. He is Head of Innovation at Lloyd’s including responsibility for horizon scanning and emerging risks. Subjects covered in recent years include: the economic and social implications of a food system shock; the effects of cyber-attacks on the US energy grid and an exploration of aggregation modelling methods for liability risks.

He is co-chairman of OASIS, an open modelling platform for catastrophe models and sits on the Board of the Lighthill Risk Network.

George Ng, a founder and Chief Technology Officer, leads major research projects and initiatives at Cyence. Previously, he was the Chief Data Scientist at YarcData. George has also worked as a Research Scientist at DARPA and US-CERT and as faculty at American University. He received his PhD from UC Irvine and B.A. from UC Berkeley, both in Economics.

Remerciements

Pour l’ensemble des remerciements merci de vous reporter au rapport complet.

Synthèse

Ce rapport a pour objectif de fournir aux assureurs devant définir des solutions d'assurance cyber, des scénarios réalistes et plausibles afin de les aider à quantifier les risques cyber. La prise de conscience à l'égard de la responsabilité informatique et de l'exposition aux risques cyber est relativement limitée en comparaison avec d'autres catégories d'assurance.

En développant leur compréhension de l'exposition aux risques cyber, les assureurs seront en mesure d'améliorer la gestion de l'exposition de leur portefeuille, de définir des limites appropriées et d'acquérir la confiance nécessaire pour s'engager sur ce segment de l'assurance en plein essor.

Le rapport s'adresse aux risk managers dont les activités sont exposées aux types de cyberattaques décrits dans les deux scénarios du rapport : une opération de piratage nuisant à l'activité de leur prestataire de services informatiques cloud ou une attaque entraînant la défaillance d'un système d'exploitation spécifique au sein de leur propre entreprise ou chez leurs clients, fournisseurs et/ou partenaires professionnels.

Chacun de ces scénarios comprend un ensemble de variables incluant l'atténuation des risques et la réponse en cas d'attaque cyber. Cela signifie que les organisations peuvent estimer l'impact sur leurs propres opérations.

Méthodologie

Ce rapport a été élaboré par Le Lloyd's et Cyence qui ont constitué une équipe pluridisciplinaire d'experts en cybersécurité, en modélisation des risques économiques et en assurance cyber.

Cyence a entrepris un processus structuré de recherche en sept étapes, afin de générer les scénarios et produire les estimations de perte dans ce rapport. Les sept étapes sont les suivantes :

1. Étude des technologies largement répandues et adoptées dans toutes les industries
2. Étude des autres facteurs non techniques
3. Collecte et traitement des données relatives aux différentes expositions
4. Analyse des voies d'accumulation d'exposition
5. Sélection des scénarios, modèles de fréquence et de gravité
6. Discussion et analyse avec les experts en assurance et en cybersécurité
7. Calcul des pertes et revue finale

Le Lloyd's a travaillé conjointement avec la Lloyd's Market Association (Association du marché du Lloyd's) sur une succession d'ateliers collaboratifs impliquant des souscripteurs du marché du Lloyd's spécialisés en assurance cyber pour échanger et inclure le retour d'information dans le rapport, ainsi que pour identifier les répercussions et les éléments d'appréciation pour le secteur de l'assurance.

Attaques cyber: une menace grandissante

Le risque cyber est une menace mondiale croissante. Alors que la technologie numérique révolutionne les modèles commerciaux et transforme la vie quotidienne, elle rend également les économies mondiales plus vulnérables face aux cyberattaques.

De ce fait, les conséquences de la cybercriminalité sur l'économie et les assurances s'aggravent. On estime qu'en 2016, les cyberattaques ont coûté quelques 450 milliards d'USD aux entreprises, à l'échelle mondiale (*Graham, 2017*). De plus en plus, les assureurs proposent une assistance dans la gestion de ces événements : il peut s'agir d'infractions individuelles causées par des initiés malveillants ou des pirates informatiques, de pertes plus conséquentes liées, par exemple, à des infractions relatives aux terminaux de points de vente, d'attaques par ransomware (telles que BitLocker et WannaCry), ou encore d'attaques par déni de service distribué comme Mirai.

La cybermenace se propage à un rythme croissant et son expansion devrait se poursuivre avec le développement numérique, dans l'économie mondiale, des opérations, des chaînes d'approvisionnement et des transactions commerciales ainsi que des services aux employés et aux clients.

Des défis à relever pour les assureurs

À mesure que la menace cyber croît, la demande en assurance cyber augmente. L'équipe Class of Business Performance du Lloyd's estime que le marché mondial de la cyberassurance représente aujourd'hui entre 3 et 3,5 milliards d'USD. D'ici 2020, certains analystes pensent qu'il pourrait peser 7,5 milliards d'USD (*PwC, 2015*). Les assureurs biens et responsabilités ont enregistré 1,35 milliard de dollars de primes directes souscrites pour la

cyberassurance en 2016, soit un bond de 35 % par rapport à 2015, d'après les rapports de Fitch Ratings et A.M. Best.

Malgré cette progression, la compréhension par les assureurs des questions de responsabilité et d'agrégation des risques en matière de cybersécurité est un processus de longue haleine qui évolue avec l'expérience et la connaissance croissantes liées aux cyberattaques. L'utilisation que les assurés font d'Internet est également en pleine évolution, occasionnant un changement rapide dans l'accumulation des risques cyber, sans précédent par rapport à d'autres menaces.

La modélisation des risques dans l'assurance traditionnelle repose sur des sources d'information fiables, telles que des données nationales ou de l'industrie mais il n'existe pas de sources équivalentes en ce qui concerne le risque cyber. Par conséquent, les données nécessaires à la modélisation de l'accumulation des risques cyber doivent être collectées à grande échelle. La collecte des données et leur mise à jour régulière sont donc des éléments clés pour mieux comprendre l'évolution de ce risque.

Approfondir la compréhension du cumul des risques cyber

Ce rapport est destiné à améliorer la compréhension des assureurs et des risk managers en matière de responsabilité et d'agrégation des risques cyber. Il permet d'analyser le cumul à travers le prisme de six tendances contribuant à la vulnérabilité numérique. Comprendre ces tendances est primordial pour maîtriser l'agrégation des risques cyber.

Ces tendances sont les suivantes:

1. Volume de contributeurs: le nombre de personnes développant des logiciels a augmenté de façon significative au cours des trente dernières années. Chaque contributeur peut potentiellement rendre le système plus vulnérable en raison du risque d'erreur humaine.

2. Volume de logiciels: outre le nombre croissant de personnes susceptibles de modifier le code des logiciels, le nombre de logiciels créés est également en augmentation. Plus de code signifie davantage d'erreurs potentielles et, en conséquence, plus de vulnérabilité.

3. Logiciel libre: le mouvement du logiciel libre et ouvert (open-source software) a abouti à de nombreuses initiatives innovantes. Cependant, un grand nombre de bibliothèques libres sont mises en ligne et, bien qu'elles soient supposées faire l'objet de contrôles en termes de fonctionnalité et de sécurité, ce n'est pas toujours le cas. Toute erreur introduite dans le code primaire peut être involontairement répercutée dans les itérations suivantes.

4. Ancien logiciel: plus un logiciel reste sur le marché, plus les individus malveillants ont le temps de détecter et d'exploiter ses vulnérabilités. De nombreux utilisateurs, particuliers et entreprises, utilisent des versions obsolètes de logiciels qui proposent pourtant des alternatives plus sécurisées.

5. Logiciel multicouche: les nouveaux logiciels sont généralement conçus à partir d'un code source antérieur. De ce fait, les phases de test et de correction sont fastidieuses et nécessitent la mobilisation de ressources considérables.

6. Logiciel « généré »: certains codes sources peuvent être générés par des processus automatisés pouvant être modifiés dans un but malveillant.

Le rapport a également recours à des scénarios visant à quantifier les dommages pouvant résulter de deux types d'incidents cyber.

Scénario 1: piratage d'un fournisseur de services informatiques cloud

Un groupe sophistiqué de hackers militants décide de perturber l'activité de prestataires de services informatiques cloud et celle de leurs clients pour attirer l'attention sur l'impact environnemental des entreprises et de l'économie moderne. Le groupe modifie de façon malveillante un « hyperviseur » qui contrôle l'infrastructure cloud. Cet acte se traduit par une panne de nombreux serveurs clients hébergés et par une interruption généralisée des services et de l'activité.

Scénario 2: attaque ciblant une faille généralisée

Dans un train, un cyberanalyste oublie son sac qui contient la copie papier d'un rapport sur une faille affectant l'ensemble des versions d'un système d'exploitation utilisé par 45 % du marché mondial. Mis en vente sur le dark web, ce document est acheté par un nombre indéterminé de malfaiteurs non identifiés qui développent des exploits[a] système et lancent des attaques sur des entreprises vulnérables en vue d'un gain financier.

[a] Le terme « exploit » désigne l'utilisation d'un élément de programme (logiciel, données ou commande) dans le but d'exploiter une faille présente dans un système d'exploitation ou un logiciel, à des fins malveillantes.

Résultats clés

Le rapport met en évidence cinq constatations majeures:

- Les impacts économiques directs des incidents cyber peuvent entraîner un grand nombre de préjudices économiques. Concernant le scénario relatif au dysfonctionnement des services informatiques cloud, mentionné précédemment dans ce rapport, ce type de dommages s'étend de 4,6 milliards d'USD pour un incident important, à 53,1 milliards pour un incident majeur. Dans le scénario d'une faille logicielle généralisée, les pertes moyennes s'échelonnent entre 9,7 milliards d'USD pour un incident important et 28,7 milliards pour un incident majeur[b].

- Les pertes économiques pourraient être nettement inférieures ou supérieures à la moyenne calculée dans les deux scénarios, leur montant global étant difficile à déterminer précisément. Ainsi, alors que les pertes moyennes dans le scénario de défaillance des services informatiques cloud s'élèvent à 53,1 milliards d'USD pour un incident majeur, elles pourraient atteindre 121,4 milliards ou se limiter à 15,6 milliards d'USD [c] en fonction, notamment, des entreprises concernées et de la durée d'indisponibilité des services.

- Les attaques cyber peuvent générer un montant assuré s'évaluant en milliards de dollars. Dans le cas du scénario de défaillance des services informatiques cloud, par exemple, le montant assuré est compris entre 620 millions d'USD pour une perte importante et 8,1 milliards pour une perte majeure. Dans le cas du scénario d'une faille logicielle généralisée, le montant assuré est compris entre 762 millions d'USD (perte importante) et 2,1 milliards (perte majeure).

- Les scénarios révèlent un déficit d'assurance compris entre 4 milliards d'USD (perte importante) et 45 milliards (perte majeure), en ce qui concerne le scénario de défaillance des services informatiques cloud, les pertes économiques étant couvertes à hauteur de 13% et 17% respectivement. Pour le scénario de la faille logicielle généralisée, le déficit d'assurance est compris entre 8,9 milliards d'USD (perte importante) et 26,6 milliards (perte majeure), seuls 7% des pertes économiques étant couverts.

- Lorsque les primes du marché estimées actuelles sont évaluées par rapport aux estimations de perte prévues par les scénarios d'assurance cyber présentés dans ce rapport, il apparaît qu'un seul incident cyber peut accroître le ratio sinistres-primes du secteur de 19% et 250% respectivement, en cas de pertes importantes et majeures. Cela illustre le potentiel catastrophique du risque cyber.

Conclusion

La demande en assurance cyber augmente à mesure que la menace cyber progresse.

Malgré cette progression, la compréhension par les assureurs des questions de responsabilité et de cumul des risques en matière de cybersécurité est un processus de longue haleine qui évolue avec l'expérience qu'ils acquièrent. Aussi, il est crucial que la compréhension du risque, y compris les calculs de primes techniques et les modèles de capital, garde le rythme face à l'évolution constante de la base de connaissances relative au risque cyber.

Dans d'autres branches d'assurance, les assureurs ont développé une meilleure compréhension en matière de responsabilité et d'agrégation des risques. Par exemple, il est largement admis que les catastrophes naturelles sont susceptibles de donner lieu à de multiples déclarations de sinistres émanant de nombreux assurés, participant ainsi à l'augmentation considérable du coût des sinistres pour les assureurs. Les polices d'assurance couvrant les catastrophes naturelles tiennent généralement compte de ce fait et la réassurance est alors communément utilisée afin de réduire l'impact du cumul des risques.

Les résultats du rapport indiquent que les pertes économiques résultant d'incidents cyber peuvent être aussi conséquentes que celles engendrées par les ouragans les plus dévastateurs. Considérer l'assurance cyber en ces termes et anticiper de façon explicite l'impact des catastrophes liées à la cybersécurité pourrait constituer un réel avantage pour les assureurs. Pour y parvenir, la collecte des données et le niveau de qualité de ces dernières sont des éléments primordiaux, d'autant plus que les risques cyber évoluent sans cesse.

Afin que le secteur de l'assurance puisse capitaliser sur le marché en pleine croissance de la cybersécurité, les assureurs pourraient tirer avantage d'une meilleure compréhension du risque volatile, implicite dans le domaine de l'assurance cyber.

Les risk managers peuvent utiliser les scénarios de cybersécurité afin d'envisager les impacts des attaques cyber sur leurs principaux processus opérationnels et mettre en œuvre les actions nécessaires pour limiter ces risques.

[b] Les chiffres cités représentent le montant moyen des pertes estimées sur une période d'un an en cas d'événement important ou majeur. Ils tiennent compte de l'ensemble des dépenses directes attendues liées à ces événements. Les conséquences de type dommages aux biens, atteintes corporelles ou encore pertes indirectes, notamment la perte de clients et l'atteinte à la réputation, ne sont pas prises en considération.

[c] L'intervalle de confiance pour ces exemples est de 95 %. Valeur considérée comme estimation fiable pour la prise en compte des paramètres connus et inconnus.

Références

Graham, L. 2017. Cybercrime costs the global economy $450 billion [en ligne] (La cybercriminalité coûte 450 milliards d'USD à l'économie mondiale). CNBC Cyber Security. Consultable sur : http://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html

PwC. 2015. Insurance 2020 & beyond: Reaping the dividends of cyber resilience [en ligne] (L'assurance en 2020 et au-delà : récolter les fruits de la cyberrésilience). Consultable sur : http://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf

Stanley, C. 2017. Évaluation du marché de la cyberassurance (Interview du 26 juin avec Christian Stanley, Casualty Executive, Class of Business Underwriting Performance, Lloyd's).