

« Le spectre des cyberrisques ne cesse de s'élargir »

Interview | 02 novembre 2022

L'un des plus grands réassureurs estime les dommages économiques causés à l'échelle mondiale par la cybercriminalité à 6000 milliards de dollars américains pour l'année 2021, soit à peu près le montant de ceux occasionnés par la pandémie et les mesures pour la combattre. Les assureurs ont un rôle important à jouer en matière de prévention et de réduction des cyberrisques, déclare l'expert de l'ASA en cyberrisques, Gabor Jaimes.

Gabor Jaimes, pourquoi les cyberrisques relèvent-ils des risques majeurs - à l'instar d'une pandémie ou d'un séisme de grande magnitude ?

Dans son « [Rapport sur les risques 2020](#) », l'Office fédéral de la protection de la population OFPP a identifié les risques qui menacent la Suisse. Il s'agit notamment de catastrophes naturelles de toutes sortes, de cyberattaques de grande envergure, de pandémies ou de pénuries d'électricité. De tels risques majeurs sont à même de provoquer des dommages économiques et immatériels immenses pour l'économie et la société. Du fait de la mondialisation et de la numérisation croissantes, certains risques majeurs peuvent avoir des répercussions bien plus conséquentes que par le passé, voire paralyser en partie notre monde interconnecté – surtout, les cyberrisques.

Les dommages économiques susceptibles d'être causés par la cybercriminalité sont estimés à quelque 6000 milliards de dollars américains à l'échelle mondiale pour l'année 2021. Un nombre astronomique – et nous savons que seule une toute petite partie d'entre eux est assurée.



Les cyberrisques ne connaissent pas de frontières cantonales ni nationales et menacent pratiquement tous les secteurs. C'est pourquoi une collaboration constructive s'impose en matière de cybersécurité, ceci à tous les niveaux : Expert de l'ASA en cyberrisques, Gabor Jaimes.

Pourquoi la lutte contre les cyberrisques passe-t-elle par l'interaction entre divers acteurs ?

En cas de cyberattaque d'envergure mondiale, nous estimons le potentiel de dommages à cent milliards de dollars américains, voire plus, au total. Les assureurs ne peuvent guère satisfaire aux couvertures requises par le marché, même en s'appuyant sur les réassureurs. De tels risques systémiques sont de surcroît en mesure de mettre en difficulté financière les assureurs et les réassureurs actifs à l'international. Pour ne pas compromettre l'indemnisation des sinistres dans d'autres domaines d'assurance, le secteur de l'assurance doit garder un œil sur ces risques et les gérer en conséquence. Néanmoins, afin d'offrir la meilleure protection possible à notre économie et à notre société, il nous faut réfléchir à des solutions en partenariat avec toutes les parties prenantes, y compris avec la Confédération. C'est la seule façon de renforcer la cyberrésilience. Celle-ci est essentielle non seulement pour notre société, mais aussi pour la consolidation durable de la place économique suisse.

Les cyberrisques constituent une branche au fonctionnement singulier. Outre des connaissances classiques en assurance, elle requiert des compétences numériques approfondies.

Quelles opportunités les cyberrisques offrent-ils au secteur de l'assurance ?

Pour les assureurs, les cyberrisques représentent un énorme potentiel de croissance. D'une part, du fait des lacunes criantes en cybersécurité et de l'ambition de nombre d'organisations et de gouvernements de mieux se protéger, c'est-à-dire d'améliorer leur résilience. D'autre part, en raison de la numérisation inéluctable de nombreux processus de la vie courante des entreprises et des particuliers. Le volume actuel des primes devrait plus que doubler d'ici 2025 – et passer de neuf à 22 milliards de dollars américains selon les estimations. Cela signifie que d'ici une dizaine d'années, la cyberassurance pourrait devenir une branche d'assurances et de réassurance à part entière dans un environnement de marché bien développé – à l'instar aujourd'hui de l'assurance de choses, de l'assurance automobile, de la responsabilité civile ou de l'assurance maladie.

Il ne faut pas sous-estimer non plus les 300 milliards de dollars américains a priori dépensés chaque année pour la cybersécurité dans le monde. Une couverture d'assurance ne pouvant exister sans prévention, nombreux sont les partenariats possibles entre les assureurs et les fournisseurs de services informatiques le long de la chaîne de création de valeur, ce qui ne manquera pas de stimuler l'innovation.

Par ailleurs, les cyberrisques constituent une branche au fonctionnement singulier. Outre des connaissances classiques en assurance, elle requiert des compétences numériques approfondies, lesquelles sont essentiellement l'apanage des jeunes générations. C'est une occasion unique pour le secteur de l'assurance d'attirer de tels talents et de se les rallier sur le long terme – tout en se donnant ainsi la chance de répercuter cette nouvelle manière de penser ou ces nouvelles approches sur d'autres domaines.

Comment fonctionne la collaboration dans celui des cyberrisques, toutes branches confondues ?

Les cyberrisques ne connaissent pas de frontières cantonales ni nationales et menacent pratiquement tous les secteurs. C'est pourquoi une collaboration constructive s'impose en matière de cybersécurité, ceci à tous les niveaux. Elle commence par le signalement le plus rapide possible de chaque incident afin d'empêcher son éventuelle propagation, par exemple celle de logiciels malveillants au sein d'une entreprise – ou, tout au moins, d'en réduire les effets. La transparence revêt alors une importance capitale, mais constitue en même temps un défi de taille : en effet, aucune entreprise n'aime reconnaître qu'elle a été victime d'une cyberattaque. C'est pourquoi cet échange d'informations doit avoir lieu en « lieu sûr », en temps réel et dans le respect de règles du jeu clairement définies.

La Confédération offre une telle plate-forme avec le [Centre national pour la cybersécurité NCSC](#). Interlocuteur à l'échelle nationale, le NCSC reçoit les signalements de cyberincidents et de failles de la part des particuliers, des entreprises, des pouvoirs publics et des spécialistes informatiques. Il est également responsable de la coordination de la mise en œuvre de la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC). Dans le cadre de l'édition 2023 de la SNPC, le secteur de l'assurance est parvenu jusqu'à présent à faire entendre ses préoccupations, raison pour laquelle il soutient cette stratégie.

Forts de cet exemple, les prestataires de services financiers se sont également regroupés pour contribuer à la cyberrésilience de manière concertée. Avec le [Swiss Financial Sector Cyber Security Centre \(FS-CSC\)](#) dont l'ASA compte au nombre des membres fondateurs, ils offrent une plate-forme pour l'échange de connaissances, la mise en réseau ainsi que la gestion des crises et encouragent la collaboration institutionnelle entre les établissements financiers et les autorités sur les aspects stratégiques et opérationnels.

L'une des missions du secteur de l'assurance réside dans la sensibilisation de sa clientèle, entreprises et particuliers, mais aussi de la société dans son ensemble, à la problématique de la cybersécurité.

Quel rôle le secteur de l'assurance peut-il jouer en matière de prévention ou de lutte contre la cybercriminalité ?

Dans le domaine de la cyberassurance, il ne suffit pas de remettre une police, garante d'une indemnisation en cas de sinistre. L'une des missions du secteur de l'assurance réside dans la sensibilisation de sa clientèle, entreprises et particuliers, mais aussi de la société dans son ensemble, à la problématique de la cybersécurité. Une autre consiste dans la mise en exergue des comportements imprudents, qu'ils soient conscients ou non. Les assureurs entendent tout d'abord veiller à ce que leurs clients disposent d'un système de défense solide – et, ensuite seulement, les aider au mieux à résister aux attaques. Idéalement, une communication diligente et partenariale permet d'isoler une situation problématique, de prévenir des dommages plus importants et de limiter une éventuelle interruption des activités.

Mot d'ordre « résilience » : de quelle marge de manœuvre disposons-nous, chacune et chacun à notre niveau, pour prévenir les cyberattaques ?

Les cyberattaquants misent souvent sur l'ignorance ou l'imprudence des collaboratrices et des collaborateurs. Ceux-ci doivent avoir pleinement conscience de leur rôle et savoir comment se protéger. Car ils sont une pièce importante du puzzle dans la lutte contre les cyberattaques. Un particulier non plus n'est pas à l'abri d'éventuelles offensives. En cas de piratage de sa messagerie privée ou de son compte bancaire, un virus peut alors se propager à l'ensemble du système. Il faut s'assurer de la mise à jour régulière des programmes et des applications ainsi que de celle de la protection antivirus. La prévention est encore la meilleure des protections. Ensuite, c'est l'assurance qui entre en jeu. Or, celle-ci ne saurait remplacer la valeur immatérielle des données perdues, par exemple dans le cas de données personnelles.

Portrait de Gabor Jaimes

Gabor Jaimes est chargé des assurances de choses, de la cyberassurance et des dommages naturels au sein de l'Association Suisse d'Assurances ASA. Fort de plus de 20 ans d'expérience dans le secteur de la réassurance, dont 15 ans environ auprès de Swiss Re. Depuis cinq ans environ, il s'intéresse de près à la cyberassurance et siège au comité de pilotage du Swiss Financial Sector Cyber Security Center (FS-CSC)

Cyberrisques

Numérisation

Risques majeurs

Vous pourriez être intéressé par ce qui suit

Add to PDF generator

Renforcer la cybersécurité sur la place financière suisse

Avec la création de l'association « Swiss Financial Sector Cyber Security Centre » (Swiss FS-CSC), la place financière suisse s'organise contre la menace croissante des cyberincidents.

News 06.04.2022

[Plus](#)

Add to PDF generator

« Plus une entreprise est numérique, plus elle est dans le collimateur »

La criminalité sur l'Internet a fortement progressé. Florian Schütz, délégué fédéral à la cybersécurité, répond aux questions les plus pressantes.

Interview 22.09.2021

[Plus](#)

Add to PDF generator

Les cyberrisques, risques émergents

Les entreprises privées comme les entreprises publiques dépendent aujourd'hui des systèmes informatiques, ceci quels que soient leurs domaines d'activité.

Emerging Risks - une évaluation du point de vue de la responsabilité civile 15.06.2022

[Plus](#)
