Swiss Re
Institute

Communiqué de presse

Malgré sa complexité, assureurs et entreprises peuvent venir à bout du cyber-risque, selon *sigma* de Swiss Re ; lancement officiel du Swiss Re Institute

- Les coûts potentiels des cyber-attaques montent en flèche ; cyber-sécurité et cyber-résilience sont de plus en plus un sujet de préoccupation pour les entreprises
- Le marché de la cyber-assurance se développe à grande vitesse, mais l'ampleur de la couverture est encore relativement modeste
- Les innovations produits et processus, ainsi que les Big Data et l'analyse intelligente, permettront d'améliorer les solutions de cyber-assurance
- Les pouvoirs publics peuvent jouer un rôle important pour accroître la cyber-résilience
- Ceci est la première étude publiée par le Swiss Re Institute, dont c'est le lancement officiel aujourd'hui

Zurich, le 1er mars 2017 – Le cyber-risque est une préoccupation croissante des entreprises, car, au vu des dernières attaques, les coûts d'une cyber-infraction peuvent s'envoler bien au-delà de la gestion des répercussions de la perte ou de la corruption de données. Selon la dernière étude *sigma* de Swiss Re « Cyber : comment venir à bout d'un risque complexe ? », les entreprises doivent faire beaucoup plus pour intégrer la cyber-sécurité dans leurs programmes de gestion des risques. Des initiatives pour accroître la cyber-résilience sont d'ores et déjà en cours. Un marché dédié à la cyber-assurance se développe rapidement, mais l'ampleur de la couverture est encore modeste par rapport à l'exposition potentielle. L'innovation des produits et des processus, ainsi que l'analyse avancée, permettront à des solutions de cyber-assurance améliorées d'émerger, repousseront les frontières de l'assurabilité et étendront la portée de la couverture. Au final, certains cyber-risques, notamment ceux liés aux sinistres catastrophiques extrêmes, pourraient être inassurables.

De récentes cyber-attaques très médiatisées montrent de manière croissante que les coûts engendrés par une faille dans la cyber-sécurité dépassent la seule gestion des répercussions de la perte ou de la corruption de données.

Darren Pain, Zurich
Telephone +41 43 285 2504

Kurt Karl, Armonk
Telephone +1 914 828 8686

Jonathan Anchen, Bangalore
Telephone +91 80 4900 2650

Investor Relations, Zurich
Telephone +41 43 285 4444

Swiss Re Ltd
Mythenquai 50/60
P.O. Box
CH-8022 Zurich

Telephone +41 43 285 2121
Fax +41 43 285 2999

www.swissre.com
@SwissRe

Les entreprises doivent maintenant tenir compte d'une atteinte potentielle à leur réputation ou à la propriété intellectuelle ainsi que d'éventuels dommages aux biens et pertes d'exploitation. Le périmètre grandissant et l'ampleur des coûts potentiels associés aux cyber-incidents reflètent l'évolution perpétuelle du paysage des cyber-risques, qui est façonné par trois puissantes dynamiques :

- l'accélération du rythme et l'extension du périmètre de la transformation digitale ;
- la multiplication des sources de vulnérabilité du fait de l'hyperconnectivité, avec la diffusion rapide des dispositifs connectés et du cloud computing, par exemple ;
- et la professionnalisation des hackers appâtés par les bénéfices économiques qu'ils peuvent tirer de cyber-attaques rondement menées.

Bien qu'elles soient de plus en plus sensibilisées aux dangers, les entreprises font généralement face aux cyber-risques en étant mal préparées. Elles sont relativement peu nombreuses les entreprises qui ont intégré la cyber-sécurité à leur gestion courante des risques. La réglementation pourrait être un catalyseur du changement : des lois sont en effet adoptées dans de nombreuses juridictions, obligeant les entreprises à introduire des dispositifs renforcés de protection des données. Par conséquent, « les entreprises – qu'elles soient grandes ou petites – doivent investir davantage dans l'architecture de cyber-sécurité si elles veulent développer des capacités robustes de gestion des risques en amont et en aval du sinistre », précise Kurt Karl, économiste en chef de Swiss Re.

Gérer un risque complexe

De nombreuses entreprises cherchent à transférer les cyber-risques à des parties tierces mieux à même de les absorber. « Un marché dédié à la cyber-assurance se développe, et un nombre croissant d'assureurs est sur les rangs pour souscrire davantage d'affaires dans cette branche de spécialités », poursuit Kurt Karl. La cyber-assurance dédiée fournit habituellement une protection de base contre les atteintes à la sécurité des données et des réseaux et les pertes associées, avec des limites de capacité qui s'échelonnent aujourd'hui dans le marché entre environ 5 millions USD et 100 millions USD. Mais certains cyber-risques importants restent largement non assurés, et l'ampleur de la couverture existante est modeste par rapport aux expositions globales potentielles des entreprises.

Une contrainte essentielle pour le développement de solutions d'assurance tient à la nature même des cyber-risques. Ils sont complexes et difficiles à quantifier, plus particulièrement à cause de l'évolution rapide de l'environnement technologique et du manque de données historiques de cyber-sinistralité pouvant servir de base à l'extrapolation d'informations concernant les pertes futures possibles. Les assureurs et les vendeurs de solutions analytiques explorent différentes approches de la modélisation des cyber-risques, dont des analyses de scénarios déterministes et des modèles probabilistes, pour essayer d'estimer les pertes potentielles engendrées par les cyber-événements. L'expérience d'autres périls, tels que les catastrophes naturelles, nous laisse espérer que les modèles seront améliorés en permanence, avec l'approfondissement des connaissances sur les facteurs de risque fondamentaux et la disponibilité accrue de données de cyber-sinistralité.

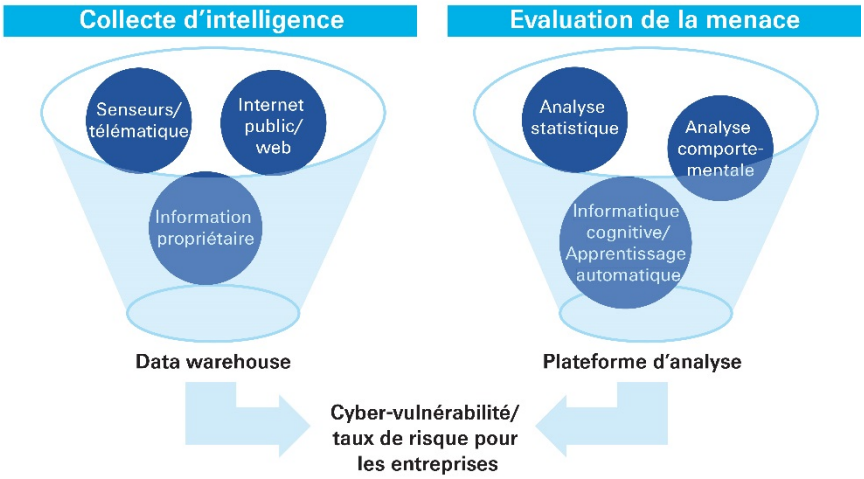
Innovation des produits et des processus

Dans l'intervalle, l'innovation produits et processus et les autres mécanismes de transfert de risque joueront un rôle important dans l'amélioration des capacités de gestion des cyber-risques. Un facteur crucial pour le rythme de l'innovation sera la capture et l'analyse de données pertinentes et de renseignements sur la menace, nécessaires pour souscrire les cyber-risques avec précision. Des initiatives sont en cours dans le secteur pour optimiser la collecte et la diffusion des informations. Par exemple, plusieurs fournisseurs d'outils d'aide à l'analyse des risques ont élaboré un schéma de données permettant aux entreprises d'identifier, de quantifier et de rapporter leur cyber-exposition aux assureurs de façon standardisée.[1] De la même manière, le CRO Forum fait la promotion d'une terminologie et d'un cadre communs pour la capture par les entreprises des informations majeures au sujet des cyber-incidents et des cyber-vulnérabilités.

Les assureurs, pour leur part, cherchent à développer des produits d'assurance flexibles, moins complexes. Il s'agit notamment aussi d'élaborer des couvertures sur mesure pour les petites et moyennes entreprises, qui ont été mal desservies par l'assurance jusqu'à présent, tout en étant souvent moins bien parées que les plus grandes firmes face aux cyber-risques. Par ailleurs, certains (ré)assureurs tentent d'établir des partenariats avec des firmes spécialisées dans la cyber-sécurité et des sociétés d'analyse de données afin de combler leurs lacunes de connaissances et de proposer des services plus complets ou additionnels à leurs clients. Plus généralement, les techniques modernes d'analyse ont la capacité « d'augmenter » les outils de souscription traditionnels des (ré)assureurs et permettent à ces derniers de réagir vite à l'évolution rapide des facteurs de risque sous-jacents.

[1] Voir, par exemple, "RMS Launches New Data Standard for Managing Cyber Insurance", *rms.com*, 19 janvier 2016, et *Verisk Cyber Exposure Data Standard and Preparer's Guide* , AIR, 2016.

Figure 1 : L'analyse intelligente : un outi de souscription complémentaire



Source : Swiss Re Economic Research & Consulting.

Un autre moyen pour augmenter la capacité dédiée à l'offre cyber est la création de véhicules d'investissement destinés à faire supporter une partie des expositions par les investisseurs sur les marchés financiers. Quelques initiatives pour créer des titres assurantiels (ILS) en couverture de risques opérationnels tels que le cyber ont cours à l'heure actuelle. Le marché des ILS pour les cyber-risques est encore naissant mais pourrait se développer.

Soutien des pouvoirs publics

Les entreprises, si elles veulent repousser les frontières de l'assurabilité, devront collaborer avec leurs assureurs à la création d'un marché qui soit soutenable. Les pouvoirs publics ont également un rôle important, qui est de promouvoir la cyber-résilience, via des mesures pour améliorer la capture et la diffusion des informations en matière de cyber, et de légiférer sur la façon dont le cyberespace doit être utilisé et protégé. En remodelant les mesures incitatives et en intensifiant la sensibilisation aux cyber-menaces, les pouvoirs publics donneraient un coup de pouce à des solutions de marché améliorées à l'initiative du secteur privé. Or, à partir d'un certain stade, l'ampleur potentielle des pertes de certains cyber-événements pourrait dépasser la capacité d'absorption du secteur privé de la (ré)assurance, notamment pour les sinistres de pointe, tels que la perturbation généralisée d'infrastructures ou de réseaux critiques, pouvant engendrer des cumuls de dommages considérables.

Ce *sigma* est le premier à être publié sous la bannière du « Swiss Re Institute ». Swiss Re Institute est officiellement inauguré le 1er mars 2017. Sa mission consiste à renforcer la position de leader d'opinion de Swiss Re au sein de l'industrie, en réunissant sous un seul toit les diverses compétences de notre firme dans les domaines de la recherche et des relations publiques. Swiss Re Institute produira les études de recherche de Swiss Re, dont *sigma*, la publication de recherche leader de l'industrie de l'assurance.

Swiss Re
Institute

Informations aux rédacteurs

Swiss Re
Le groupe Swiss Re est un prestataire global leader en matière de réassurance, d'assurance et d'autres formes de transfert de risqué fondées sur l'assurance. Il opère directement ou par l'intermédiaire de courtiers. Sa base de clientèle mondiale se compose de compagnies d'assurance, de grandes et moyennes entreprises ainsi que de clients du secteur public. Grâce à sa solidité financière, son savoir-faire et sa force d'innovation, Swiss Re propose une gamme de solutions allant de produits standard aux couvertures sur-mesure dans toutes les branches d'assurance, facilitant ainsi la prise de risque dont dépendent l'activité entrepreneuriale et le progrès dans la société. Fondé en 1863 à Zurich, en Suisse, Swiss Re offre ses services à ses clients en s'appuyant sur un réseau d'environ 70 représentations à travers le monde. Il est noté « AA- » par Standard & Poor's, « Aa3 » par Moody's et « A+ » par A.M. Best. Les actions enregistrées de la société holding du groupe Swiss Re, Swiss Re Ltd, sont cotées au Main Standard de la SIX Swiss Exchange et négociées sous le symbole SREN. Pour plus d'informations sur le groupe Swiss Re, veuillez consulter : www.swissre.com ou suivez-nous sur Twitter @SwissRe.

Comment commander cette étude *sigma* :
La version électronique de l'étude *sigma* N° 1 /2017, *Cyber : comment venir à bout d'un risque complexe ?* est disponible en français, en anglais, en allemand et en espagnol sur le site internet de Swiss Re : www.swissre.com/sigma

La version imprimée de l'étude *sigma* N° 1/2017 en français, en anglais, en allemand et en espagnol est disponible dès à présent. Les versions chinoise et japonaise suivront prochainement. Veuillez adresser toute commande, en mentionnant vos coordonnées complètes, à sigma@swissre.com