

Le cyber risk, grand oublié de la relation Assurances- Entreprises

Guenièvre Antonini
consultante senior pour le cabinet de conseil Groupe Square



Alors que les entreprises et leurs assureurs peinent à trouver des stratégies adaptées, le coût estimé de la délinquance cybernétique pour l'économie mondiale a atteint 600 milliards de dollars en 2018, contre 445 milliards en 2014.

Les 6 et 8 février se sont tenus les Rencontres du Risk Management AMRAE à Deauville. Au programme des sujets de réflexion sur les évolutions de l'assurance, le cyber risk sur les risques numériques et informatiques tient une place importante.

Le marché de l'assurance doit faire face aux nouveaux défis que posent les avancées technologiques avec le développement croissant des cyberattaques. Le coût estimé de la délinquance cybernétique pour

l'économie mondiale a atteint 600 milliards de dollars en 2018, contre 445 milliards en 2014(1).

Alors que le risque cyber ne cesse de croître, les modalités de son assurance sont encore en phase d'ajustement. Les entreprises sont en première ligne de ce nouveau combat que représente la gestion du risque cyber.

Les entreprises et leurs assureurs peinent à trouver

des stratégies adaptées.

La cyberattaque représente l'une des crises les plus graves qui menacent les entreprises. Dans son baromètre annuel des risques, Allianz place les incidents cyber juste derrière l'interruption d'activité dans son classement mondial des risques d'entreprise(2).

De plus en plus fréquents, les incidents de sécurité des réseaux et des systèmes d'information, tels que des défaillances techniques et des virus, affectent sérieusement les entreprises allant jusqu'à perturber leur continuité d'activité.

A la grande diversité des typologies d'attaque, s'ajoute le fait que tous les incidents ne sont pas détectables, certaines entreprises pouvant être victimes d'une attaque sans nécessairement s'en apercevoir.

Il est d'autant plus complexe de mettre en place des stratégies de prévention et d'indemnisation lorsque les attaques concernent un pillage des données clients.

Les entreprises doivent alors constamment perfectionner leurs connaissances en cybernétique et renforcer leur capacité de gestion des crises. Les investissements dans les systèmes de protection sont de plus en plus coûteux(3).

Ces dernières années, les grandes entreprises mènent régulièrement des campagnes de sensibilisation auprès de leurs employés pour prévenir les risques.

De nouvelles offres émergent pour les entreprises. En novembre 2018, le groupe mutualiste FM Global spécialisé dans les risques industriels a lancé un outil interactif en ligne permettant aux entreprises d'évaluer leur niveau de maturité en cybersécurité.

Le manque de maturité du produit de cyber assurance

Le manque de maturité des produits de cyber assurance se traduit par une faible gestion du risque par les assurés en raison d'une connaissance insuffisante d'un risque récent et très évolutif. Par sa

nature même le risque de cyberattaque est difficile à évaluer, rendant le calcul de la prime d'assurance particulièrement complexe, d'autant plus que les données statistiques sont relativement récentes. L'interdépendance systémique du risque soulève le problème de trouver les cadres des responsabilités et de définir les limites des impacts d'une faille numérique.

Dans ce contexte, la question de la pertinence d'un produit d'assurance spécifiquement dédié aux risques cyber se pose encore. D'ailleurs, l'une des présentations du programme de l'AMRAE énonce clairement : « Une grande assurance Dommage ne serait-elle pas la réponse pour gérer le Cyber sur le modèle spatial ? ».

Pour que le marché de la cyber assurance se développe, il semble nécessaire d'accroître l'expertise chez les assureurs et les réassureurs. L'environnement réglementaire doit également être consolidé.

En attendant, les produits de cyber assurance sont un investissement de plus en plus utile aux entreprises qui reconnaissent que la cyber sécurité contribue à la productivité professionnelle.

L'assurance des cyber risques invite à repenser l'économie du risque à l'ère de la révolution digitale qui rend quasiment impossible la détermination de la responsabilité des risques.

En définitive, on peut se demander si la gestion du risque est encore possible.

1 Center for Strategic and International Studies, Economic Impact of Cybercrime.

2 <https://www.agcs.allianz.com/global-offices/france/news-press-france/barometre-des-risques-2019-dallianz-les-incident-cyber-rejoignent-pour-la-1ere-fois-linterruption-dactivite-en-tete-des-risques-dentreprise-dans-le-monde/>

3 https://www.accenture.com/t20170926T072837Z_w_us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

<https://notre-siecle.com>