6.6. S’assurer contre les risques cyber : oui, mais quand ?

L'assurance du risque informatique n'est pas nouvelle mais le marché de la couverture en assurance du risque cyber ne s'est réellement développé qu'aux alentours de 2013. Précédemment, la couverture était principalement destinée à la couverture du matériel informatique mais rapidement les entreprises ont pris conscience que la valeur de leur système informatique n'étant pas tant liés à leur infrastructure matérielle mais à leur contenu, les données quelles qu'elles soient : données de salariés, clients, données métiers...

À cette période, le marché est très largement capté par les trois plus importants assureurs nord-américains (AIG, Chubb et Beazley) de ce segment encore considéré comme une niche. Moins de cinq années plus tard, ce sont plus de 20 acteurs qui ont ouvert leur souscription sur ce type de produits.

À compter de 2018, les entreprises souhaitant souscrire ce type de protection n'ont désormais plus d'excuse : la très grande majorité des assureurs dispose d'une offre cyber qui peut être souscrite seule ou en extension d'autres couvertures d'assurance telles que la responsabilité civile, le dommage ou encore la fraude.

Pour autant, les assureurs ne sont pas plus à l'aise en 2018 à souscrire ce risque qu'ils ne l'étaient cinq ans auparavant, comment expliquer un tel appétit sur un risque en permanente évolution et encore peu mature ?

AUGMENTATION DE LA SINISTRALITÉ REPORTÉE AUX ASSUREURS

Si les attaques cyber ne sont pas nouvelles, la collecte de données par les assureurs reste directement corrélée au taux d'équipement de leurs assurés qui était encore très faible jusqu'alors. Ceci étant dit, les assureurs ne résonnent pas en volume de sinistres mais en rapport de sinistralité à primes souscrites. Or, le volume de primes ayant augmenté plus rapidement que celui des sinistres, ces ratios s'améliorent au fur et à mesure des années de souscription. Le ratio du rapport Sinistres à Primes aux USA se situe à 32,4% en 2017 alors qu'il atteignait 47,6 % un an plus tôt. Les assureurs comptent également sur le gain en maturité de leurs assurés, soit volontairement soit sous la pression réglementaire. A l'image d'AXA qui s'est adjoint les services de la plateforme Security Scorecard, les assureurs complètent leur connaissance du risque cyber tant pour garantir la qualité de leur souscription (assurabilité et tarification) que pour développer des services de conseil en cyber sécurité. Il en est de même pour les courtiers qui s'adjoignent les services de sociétés spécialisées.

Tout comme il est d'usage dans les branches de dommages aux biens, les assureurs ont tout intérêt à pousser leurs assurés à adopter des démarches de prévention. A la clé pour les entreprises clientes, une meilleure intégration de leur police d'assurance cyber dans leur politique globale de gestion de ce même risque. En effet, la police cyber n'est pas uniquement une protection financière du bilan de l'entreprise en cas de sinistre, les assureurs articulent les garanties autour de services, disponibles 24/24h et 7/7 j soit auprès de plateformes détenues en propre par l'assureur (notamment AXA ou AIG) ou sous-traitées à des sociétés spécialisées (par exemple, le réseau d'expert Craw-ford auquel fait appel l'assureur Chubb). Ces plateformes jouent à la fois le rôle de tri des incidents (selon l'assureur AIG qui répertorie une déclaration de sinistre par jour en 2017, 80% d'entre elles sont catégorisées comme des incidents susceptibles d'être gérés dans les 72 premières heures après notification) et de mise en relation avec des prestataires spécialisés (investigation technique, conseil juridique, conseil en gestion de crise ou communication, ...) selon le cas de figure.

PATIENCE ET PÉDAGOGIE DOIVENT GUIDER PLUS QUE JAMAIS LES ACTIONS DES COURTIERS

Si, comme le précise le baromètre 2017 mené par The Risk Management Society (l'association des professionnels du management des risques), 83 % des entreprises bénéficiaient d'une couverture cyber en 2017, il aura fallu au marché américain plus de 10 ans et des premières souscriptions réellement initiées vers 2006 pour arriver à ce taux d'équipement.

Certes, le risque de réclamation de tiers a été significativement renforcé par la médiatisation autour de la transposition du Règlement Général pour la Protection des Données (RGPD) mais la Belgique - et l'Europe en général - demeurent moins litigieuses que les Etats-Unis.

Mais l'une des principales raisons de la réticence à la souscription est la méconnaissance de son propre risque et de l'impact sur son organisation en cas d'événement majeur tel que Wannacry ou Petya.

Les entreprises attendent donc des exemples concrets. Il peut s'agir de cas reportés mais aussi de retour d'expérience de leurs courtiers dans la gestion des sinistres ou de témoignages de leurs pairs. A cet effet, il faut souligner l'effort de TV5 Monde, ou plus récemment Saint-Gobain, d'avoir communiqué sur les conséquences des attaques dont elles ont été victimes et qui ont clairement éveillé les consciences des dirigeants.

Le critère financier est bien évidemment déterminant dans l'arbitrage entre l'investissement à réaliser pour la protection des systèmes d'information et l'achat d'une nouvelle couverture d'assurance.

En outre, alors que certains assureurs n'exigent que quelques cases à cocher sur un formulaire en ligne, plus la taille du souscripteur sera importante, plus le niveau d'information requis par le ou les assureurs sollicités sont invasifs et susceptibles de constituer un frein à la souscription.

li est du devoir des courtiers d'activement poursuivre auprès des entreprises leur rôle de sensibilisation, de conseil et d'intermédiation avec les assureurs afin de les aider à sauter le pas et à profiter des meilleures conditions d'un marché d'assurance porteur. La couverture d'assurance cyber trouve aujourd'hui totalement sa place dans la politique de cyber résilience des entreprises. Il s'agit certes d'un investissement pour elles mais qui s'inscrit dans une démarche inéluctable de management de ce risque. Cela au même titre que l'on n'imaginerait plus avoir un réseau informatique sans pare-feu ou antivirus à jour.

Laurent Rondeaux
Senior Client Manager Aon Risk Solutions
AON BELGIUM
AIHE REVUE NR. 218 AOÛT-SEPTEMBRE 2018