

Les défis de la (ré)assurance cyber

Le cyber demeure un risque particulièrement exigeant à porter notamment en raison de sa nature systémique et contagieuse. La concentration des dépendances technologiques cloud, infrastructures critiques et grands fournisseurs informatiques combinée à l'interconnexion croissante des chaînes d'approvisionnement numériques, expose les assurés comme les porteurs de risque à des scénarios de pertes de grande ampleur.

Ceux-ci peuvent affecter des groupes internationaux tels que Marks & Spencer ou Jaguar Land Rover, ainsi que l'ensemble de leur écosystème (partenaires, fournisseurs et sous-traitants notamment), souvent composé de TPE/PME¹.

Cette dimension catastrophique (« CAT ») influence fortement l'appétit et la capacité des (ré)assureurs. Malgré des progrès rapides en matière de modélisation, les mécanismes de diffusion du risque évoluent plus vite que les référentiels historiques, imposant une gestion plus dynamique des expositions.

D'un point de vue de la sinistralité, le rançongiciel (ransomware) reste la principale source de pertes pour les (ré)assureurs, dans un contexte marqué par la montée en puissance d'autres scénarios tels que les attaques de la chaîne d'approvisionnement (notamment informatique) et la fraude (notamment par e-mail et par ingénierie sociale). L'intelligence artificielle joue ici un rôle de catalyseur, augmentant la fréquence et la complexité des attaques tout en contribuant également à l'amélioration des capacités de défense et de détection.

Parallèlement, les déclencheurs de sinistres cyber sont de plus en plus liés à des événements accidentels ou opérationnels (pannes cloud ou erreurs de configuration d'un logiciel par exemple) affectant des acteurs majeurs de l'écosystème numérique auxquels les assurés sont fortement dépendants. Les incidents impliquant des fournisseurs tels qu'AWS (cloud) et CrowdStrike (cybersécurité) en sont de parfaites illustrations. Cette évolution appelle une réponse adaptée de la part des (ré)assureurs aux besoins de leurs clients.

Un défi supplémentaire, souvent sous-estimé, réside dans la simplification et l'harmonisation du marché. La complexité de certains libellés contractuels (pertes d'exploitation contingentes, cyber guerre ou encore infrastructures externes) ainsi que la densité de certains questionnaires demeurent des freins à l'adoption et à la diffusion du produit, en particulier auprès des TPE/PME. Cette complexité limite également la capacité des intermédiaires (courtiers, agents et agences de souscription) à promouvoir plus largement ces solutions. Rendre l'assurance cyber plus accessible favoriserait ainsi une meilleure adhésion des assurés et permettrait aux intermédiaires d'engager plus facilement ce sujet avec leurs clients.

Face à ces contraintes structurelles, le marché cyber n'est toutefois pas resté immobile. Sous la pression conjuguée de l'émergence de nouvelles menaces, de la visibilité croissante des incidents et des exigences réglementaires, il a engagé une phase de transformation rapide, marquée par une montée en maturité des modèles, des produits d'assurance et de réassurance.

