PERSPECTIVES

Assurance cyber – Comprendre et évaluer la menace pour bâtir une assurance forte

Mai 2023

Alors que la criticité du risque cyber est maintenant à l'esprit de l'ensemble des acteurs économiques, la complexité technique de ce risque et les constantes évolutions de la menace rendent encore difficile la création de produits d'assurance adaptés aux besoins des assurés et rentables pour les assureurs.

Au regard des enjeux parfois vitaux auxquels se trouvent confrontés les acteurs du marché, il est nécessaire de répondre à cette question ardue de l'assurabilité du risque cyber. Pour ce faire, connaissance de la menace et quantification financière doivent pouvoir se conjuguer pour bâtir des scénarios crédibles sur lesquels fonder les modèles d'assurance qui permettront aux parties prenantes de s'accorder.

Accuracy associe ses compétences en modélisation financière avec la technologie de quantification du risque tirée d'une analyse dynamique de la menace cyber de Citalid, afin d'éclairer la prise de décision de ses clients dans cette démarche clé.

—

Apparu au début des années 2000, l'assurance cyber a fortement évolué passant de la couverture des risques liés aux virus et aux pertes de données, à la responsabilité civile et aux pertes d'exploitation.

Si le marché mondial de l'assurance du risque cyber, représentant aujourd'hui environ 9 milliards de dollars, est essentiellement capté par le marché américain, le même risque cible pourtant les acteurs européens qui, par conséquent, ont les mêmes besoins en assurance. Pourtant, la forte sinistralité de l'année 2020 dans un contexte d'assiette d'assurés très étroite a conduit les assureurs à un durcissement généralisé des conditions, voire le retrait pur et simple de certaines offres. En 2021, le marché français du risque cyber a représenté environ 220 millions € de chiffre d'affaires, soit 3,1% des cotisations de l'assurance des dommages aux biens des professionnels évaluées à 7 milliards € sur la même période et 0,35% du chiffre d'affaires des assurances de biens et responsabilité. Cette faible couverture ne s'est étendue qu'à seulement 0,2% des PME contre 9% des ETI et 84% des grands groupes. Or, les PME sont les entreprises les plus exposées au risque, les indicateurs disponibles tendant à montrer que 60 % des PME font faillite dans les 18 mois qui suivent une cyberattaque.

Le besoin est bien présent, mais de nombreux éléments viennent retarder l'émergence de l'assurance cyber.

En premier lieu, les cyberattaques paraissent difficiles à prédire et à comprendre. Elles peuvent en effet être menées de manière très sophistiquée et les modes opératoires sont en constante évolution. La modélisation de scénarios de risque crédibles est par conséquent un exercice complexe.

Ensuite, le coût des dommages causés par une cyberattaque est parfois considérable et inclut souvent des pertes financières, des pertes de propriété intellectuelle, des violations de données personnelles, des pertes de réputation, etc. La quantification financière des scénarios de risque se trouve fortement compliquée de la multiplicité des paramètres.

De plus, les réglementations en matière de cybersécurité varient d'un pays à l'autre, rendant difficile la création de produits d'assurance standardisés pour les entreprises internationales. Les assureurs doivent également se conformer aux réglementations en matière de protection des données personnelles, ce qui peut les rendre plus vulnérables aux poursuites judiciaires en cas de violation de la vie privée.

Enfin, la maturité cyber des entreprises sollicitant une assurance dépend de nombreux facteurs, notamment de leurs systèmes informatiques, de leurs politiques et procédures internes, mais aussi des comportements des utilisateurs de leurs systèmes. L'évaluation de ces critères, en elle-même complexe, se trouve souvent freinée par la réticence naturelle des entreprises à divulguer les détails de leur infrastructure informatique et de leurs politiques de sécurité. Déterminer le niveau d'exposition au risque et les primes d'assurance pertinentes n'est donc pas un exercice standardisé.

Par conséquent, alors que le marché de l'assurance cyber peine à trouver son modèle face à un risque aux contours et à l'impact difficilement appréciables, à une assiette d'assurés en construction et un environnement réglementaire mouvant, il est urgent d'apporter un éclairage par des scénarios de risque crédibles et des quantifications financières fondées. C'est l'objet du travail proposé par Accuracy en partenariat avec Citalid, qui vise à identifier des scénarios d'attaques en spécifiant leur fréquence et l'amplitude des pertes encourues, au regard de la vulnérabilité de l'entreprise caractérisée grâce à l'analyse de sa maturité cyber et du marché sur lequel elle évolue.

Les informations, objectives et quantifiées, tirées de ce travail ont pour finalité de permettre à l'entreprise en recherche d'assurance ou souhaitant évaluer la qualité de sa couverture d'identifier la solution la plus adaptée à sa configuration propre. A l'inverse, du côté assureur elles contribuent à la construction d'offres pertinentes et pérennes, ainsi qu'à l'évaluation de l'assurabilité des dossiers des clients.

Contact

Arthur Couvreur
Directeur
arthur.couvreur@accuracy.com
+33 6 66 69 65 15

Les associés et les professionnels d'Accuracy sont disponibles pour discuter de vos besoins et concevoir une solution adaptée avec les experts compétents.