Capgemini invent

LE RISQUE CYBER EST-IL INASSURABLE ?

La logique voudrait que l'on assure les risques du monde virtuel au même titre que ceux du monde réel. Pourtant, à mesure que le risque cyber grandit, les sociétés d'assurances s'interrogent sur leur capacité à fournir un service d'indemnisation qui soit à la hauteur des pertes potentielles en cas de cyber-attaque ou cyber-incident. « Le volume d'indemnisation des sinistres a été multiplié par trois entre 2019 et 2020, amenant le ratio sinistres/primes à 167% contre 84% un an plus tôt » selon un récent article de l'Usine Digitale. Les assureurs ont d'ailleurs fait shifter leur modèle de prime vers des activités de prévention plutôt que de protection pure. Alors faut-il assurer le risque cyber ?

LA CYBERSÉCURITÉ, UN RISQUE PAS COMME LES AUTRES

Le risque cyber présente plusieurs particularités. Contrairement à un dommage sur un bien ou une personne, le risque cyber est une tache d'huile : au premier abord il impacte des systèmes et peut bloquer la livraison de services ou produits, mais bien au-delà, il peut avoir des conséquences sur la réputation et entraîner une perte de parts de marché, une baisse en bourse ou une perte de confiance. Les 250 millions de dollars de perte annoncés par le Groupe St Gobain suite à l'attaque NotPetya de 2017 ne sont pas liés uniquement aux coûts de réparation : ils incluent des pertes et arrêts sur les périmètres de l'IT et de l'industrie, impactant directement les métiers. Bien plus difficile à anticiper et à chiffrer, ils ont entraîné des répercussions comme la diminution drastique des ventes et des parts de marché. Faut-il assurer le risque cyber au-delà des coûts de réparation IT ?

Par ailleurs, contrairement à un constat classique, les cyber-victimes peuvent influencer le niveau de gravité du cyber-sinistre entre son déclenchement et sa clôture : elles peuvent déployer des actions qui limiteront ou, au contraire, aggraveront les conséquences de l'attaque en fonction de la performance de sa gestion de crise. Sans compter que les bonnes pratiques de gestion de cybercrise peuvent être contradictoires avec les intérêts des assureurs : comme soulevé par Guillaume Poupard, Directeur Général de l'ANSSI (Agence nationale de la sécurité des systèmes informatiques) en 2021, « le jeu trouble de certains assureurs » pousse les cyber-victimes à payer la rançon demandée par les cybercriminels. Le texte d'orientation et de programmation du Ministère de l'Intérieur publié le 16 mars fait débat à ce sujet puisqu'il pourrait indirectement légaliser le paiement de ces cyber-rançons.

Enfin, le risque cyber est un domaine d'expertise à part entière. Gérer, quantifier et maîtriser un risque cyber nécessite de connaître (en temps réel !) l'état de la menace, et de comprendre les aspects à la fois managériaux et opérationnels de la sécurité numérique. Cette haute professionnalisation des assureurs soulève une question de modèle métier. Arnaud Gressel, fondateur de RESCO Courtage et Auditeur INHESJ rappelait récemment qu'« il va y avoir de belles alliances à réaliser en matière de synergie des compétences » entre les assureurs et les acteurs de la sécurité pour pouvoir délivrer un service d'assurance cyber. Pour définir le niveau de risque encouru, les assureurs s'appuient de plus en plus sur des expertises externes, incluant les agences de rating.

Du côté de l'assuré cette fois, se pose la question de l'évaluation de sa maturité cyber et des actifs à assurer en priorité. La difficulté du marché de la cyber assurance est d'accoster la vision des assurés et celle des assureurs pour déterminer le rapport prime/indemnisation.

DES MODÈLES DE CYBER-ASSURANCE DIFFICILES À INDUSTRIALISER

Assurer contre la cybercriminalité pourquoi pas mais faut-il assurer le risque cyber pour tout type de victimes ? Les cyber-victimes peuvent être des individus, des petites entreprises ou des grands comptes. L'étude LUCY de l'AMRAE publiée l'année dernière rapporte que 87% des grands comptes sont assurés contre 8% seulement des plus petites entreprises (TPE/PME). La compréhension et la maîtrise des enjeux de sécurité numérique varient considérablement que l'on soit une grande organisation avec des services de sécurité structurés, financés et régulièrement audités, ou que l'on soit un plus petit acteur assez peu formé aux technologies de l'information et aux enjeux de sécurité.

Les assureurs sont également touchés par des questions de déontologie : assurer le risque lié aux données personnelles par exemple peut-être mal perçu. La protection des données à caractère personnel est régie par les institutions nationales et internationales, tout manquement est puni (financièrement) par la loi : assurer ce risque reviendrait à assurer des utilisateurs de transports publics contre le risque d'amende en cas de fraude. Les assureurs doivent imaginer des business models différents en fonction des types d'acteurs et des types de risques.

Les actualités de l'assuré peuvent aussi déterminer le besoin et la granularité de l'assurance. Dans certains contextes comme les fusions / acquisitions, il y a une forte incertitude sur le niveau de maturité cyber de l'entité acquise et de celui qui résultera de l'opération – sans compter que les moments de transition sont particulièrement ciblés par la cybercriminalité qui cherche à exploiter une vulnérabilité conjoncturelle. Le Jour 1 de fusion est un moment de cyber-tension. Depuis l'arrêt de la Cour de cassation du 25 novembre 2020, la responsabilité pénale et administrative d'une société peut être engagée en raison d'actes accomplis par la société absorbée avant la fusion : doubler de vigilance et d'assurance dans ces temps forts est indispensable. Précisons la question de départ à nouveau : faut-il assurer le risque cyber ponctuellement ?

RENTABILITÉ *VERSUS* SOUVERAINETÉ

Face à ces logiques de rentabilité business des assureurs, émerge une préoccupation de souveraineté numérique. Faut-il assurer le risque cyber *en Europe ?* Assurer une organisation nécessite de manipuler des informations confidentielles sur son patrimoine et son niveau de maturité. Régionaliser les offres de cyber-assurances pourrait avoir un sens pour protéger des secrets d'intelligence économique et géopolitiques. D'autant plus que l'assureur peut être soumis à une réglementation applicable à son pays d'origine, parfois contradictoire avec celle de l'assuré.

Plus largement, assurer le risque cyber devient une forme d'engagement et de puissance régionale. Il pourrait devenir important de développer des assureurs best *players* en Europe, démontrant une fiabilité long-terme aux assurés et évitant de fragmenter les efforts aux niveaux nationaux. Pour autant, faut-il assurer le risque *de cyber-guerre ?* La guerre en Ukraine inquiète les (ré)-assureurs bien incapables d'indemniser des dommages systémiques.

Bien au-delà des risques de cyber-attaque traditionnels, l'arrivée de nouvelles tendances technologiques telles que le développement du métavers pose la question d'assurer de nouveaux types de produits virtuels achetés (ex. NFT) et d'indemniser les victimes de *hacking*. Le cas du galeriste Todd Kramer qui a perdu 2,2 millions de dollars de NFT suite à une attaque par phishing en est un cas d'étude emblématique. A défaut d'assurer ces produits, les assurances pourraient avoir un rôle de sensibilisation autour de ces nouveaux risques.

Auteurs

Jeanne Heuré
Head of Digital Trust & Cyber - Capgemini Invent

Julien Assouline
Head of Invent Financial Services South Central Europe - Capgemini Invent

A propos de Capgemini Invent

Capgemini Invent est la marque d'innovation digitale, de design et de transformation du groupe Capgemini, qui permet aux dirigeants de façonner l'avenir de leurs entreprises. Etablie dans plus de 36 bureaux et 37 studios de création dans le monde, elle comprend une équipe de plus de 10 000 collaborateurs composée d'experts en stratégie, de data scientists, de concepteurs de produits et d'expériences, d'experts en marques et en technologie qui développent de nouveaux services digitaux, produits, expériences et modèles d'affaire pour une croissance durable.

Capgemini Invent fait partie du groupe Capgemini, un leader mondial, responsable et multiculturel, regroupant 340 000 personnes dans plus de 50 pays. Partenaire stratégique des entreprises pour la transformation de leurs activités en tirant profit de toute la puissance de la technologie, le Groupe est guidé au quotidien par sa raison d'être : libérer les énergies humaines par la technologie pour un avenir inclusif et durable. Fort de 55 ans d'expérience et d'une grande expertise des différents secteurs d'activité, Capgemini est reconnu par ses clients pour répondre à l'ensemble de leurs besoins, de la stratégie et du design jusqu'au management des opérations, en tirant parti des innovations dans les domaines en perpétuelle évolution du cloud, de la data, de l'Intelligence Artificielle, de la connectivité, des logiciels, de l'ingénierie digitale et des plateformes. Le Groupe a réalisé un chiffre d'affaires de 18 milliards d'euros en 2021.

*Get The Future You Want**

Plus d'informations sur www.capgemini.com/invent

** Capgemini, le futur que vous voulez*