Innovations assurantielles au service de la lutte contre le risque cyber

CAROLINE HILLAIRET,

Professeure à l'ENSAE Paris, CREST, et Membre certifié de l'Institut des actuaires

OLIVIER LOPEZ,

directeur de l'ISUP, Sorbonne Université et Membre agrégé de l'Institut des actuaires

Le risque cyber désigne l'ensemble des risques liés à l'usage des technologies numériques. Avec la croissance de l'économie digitale, il est devenu aujourd'hui un risque économique majeur, avec des incidents cyber en forte augmentation, et des coûts, directs et indirects, estimés à environ 1% du PIB mondial c'est-à-dire de l'ordre de mille milliards d'euros par an (cf. (1)).

Le secteur financier est particulièrement concerné par le risque cyber : d'après le président de la Réserve Fédérale américaine Jerome Powell, le risque cyber constitue la principale menace pesant sur le système financier mondial. En effet ce secteur, qui est fortement numérisé et interconnecté, est une cible privilégiée pour les hackers, d'autant plus qu'il présente des gains potentiellement importants pour les cyber-pirates. Il peut ainsi se trouver en situation de victime contaminée par la crise, et doit se préparer à des attaques majeures, et notamment à de potentiels événements d'une ampleur systémique.

Le secteur de la finance et de l'assurance est aussi bien sûr fournisseur de solutions de couverture du risque et a un rôle important à jouer pour contribuer à la résilience de l'économie et de la société face au risque cyber. Ainsi le marché de la cyber-assurance s'est développé, en mettant en avant des offres innovantes qui couplent prévention, réparation financière, et accompagnement en cas de crise. Néanmoins, de nombreuses questions se posent sur leur viabilité, et sur la capacité du secteur à mutualiser les pertes en cas de sinistre majeur, comme l'illustre le récent rapport LUCY de l'AMRAE (2).

Face à ce risque de grande ampleur, la question de son assurabilité est liée à une éventuelle perte de mutualisation. La mutualisation, mécanisme au coeur de l'assurance, repose sur la compensation du coût des sinistres par les bons résultats sur le reste du portefeuille. Plusieurs caractéristiques du risque cyber peuvent la mettre en péril, notamment le caractère à la fois catastrophique et systémique de ce risque. Un événement catastrophique, touchant une seule victime, peut atteindre des montants trop importants avec probabilité trop élevée (on parle de montant de sinistres à queue de distribution lourde). Un événement systémique peut entraîner des sinistres simultanés pour un grand nombre d'assurés et engendrer un risque d'accumulation. Cette perte de mutualisation est d'autant plus accentuée si le nombre d'assurés n'est pas suffisant pour amortir les sinistres.

Face à ces écueils, un des enjeux est tout d'abord de parvenir à un équilibre entre restreindre le périmètre d'indemnisation (notamment en réduisant la capacité maximale de prestation) et la nécessité de concevoir des polices suffisamment attractives pour élargir la base de mutualisation. Dans le cas d'événements extrêmes touchant simultanément de nombreux assurés, et non mutualisables pour un assureur, des solutions de

transfert de risque adaptées au cyber doivent être développées.

Pour certaines couvertures assurantielles présentant des risques d'accumulation, comme les risques de catastrophes naturelles, des régimes spécifiques d'indemnisation, sous forme de partenariat public privé, ont été instaurés et délivrent aux assureurs une couverture de réassurance illimitée, bénéficiant de la garantie de l'Etat. L'extension de ce type de régime au cyber ne va pas de soi. On ne peut donc faire l'économie d'une réflexion autour d'autres stratégies de transfert de risque, qu'elles soient portées par un réassureur traditionnel, ou dans la perspective de constitution de captives par les grandes entreprises. La question est bien sûr d'évaluer la viabilité économique de ces stratégies. Or cette évaluation est complexe, le risque cyber étant difficile à quantifier, à la fois en raison de son périmètre évolutif et de l'absence de données fiables et structurées sur les incidents.

Bien que permettant une mutualisation à plus grande échelle, la réassurance a des limites : un événement majeur se propageant à une grande échelle dans un phénomène de contagion, et ce même au-delà des frontières, peut ainsi faire porter une charge trop importante sur le réassureur. La construction de scénarios stochastiques de crise (cf. (3) et (4)) permettrait de disposer d'un spectre très large de stress tests afin d'étudier l'impact potentiel d'un événement cyber massif et d'estimer la capacité de l'entité (assureur/réassureur/grandes entreprises) à absorber un choc d'ampleur significative.

Parmi les autres stratégies de transfert de risque, l'assurance paramétrique peut apparaitre comme une solution prometteuse pour se couvrir contre certains risques. Le déclenchement du paiement étant lié à la simple constatation de la valeur d'un indice préalablement défini, l'indemnisation se passe d'une démarche d'expertise et d'évaluation des coûts. Outre l'ouverture possible vers une titrisation, la couverture paramétrique est prometteuse car répondant à un impératif de fluidité de la compensation assurantielle. Pour l'assureur, la charge de gestion de sinistre est réduite à la portion congrue : le versement de la prestation est accélérée, favorisant ainsi une reconstruction précoce. Ce changement d'échelle temporelle dans la résolution de l'équation financière est en adéquation avec la réalité du cyber, où la plasticité de la menace impose des réactions toujours plus rapides.

Encore faut-il que le paramètre considéré réponde bien aux attentes de l'assuré. En particulier dans le contexte d'un risque perçu comme immatériel, car la réalité physique du paramètre est rarement évidente, même pour un initié. Sans doute la question ne se pose-t-elle pas de la même manière pour tous les pans du cyber. Car le cyber recouvre des phénomènes variés, avec des conséquences très disparates d'une victime à l'autre. Dans le cas d'une fuite de données, on est prêt à admettre que le volume de données dérobées est un marqueur de la perte financière associée. Le temps d'interruption d'activité d'un site de vente en ligne est également corrélé à la perte financière lors d'une attaque par déni de service. Mais même ici, ces deux propositions de paramètres sont discutables : la nature des données, les conséquences de leur fuite sont variables d'un secteur d'activité à un autre ; si une activité est dépendante de cycles saisonniers, elle peut être ponctuellement plus vulnérable - on pense par exemple à un site de vente en ligne touché rendu indisponible au moment du Black Friday.

Face à la complexité de la discussion autour du paramètre, la confiance est essentielle. Confiance en la fiabilité du paramètre, sa disponibilité et sa traçabilité. Confiance également entre assuré et assureur dans la co-construction de ce modèle d'assurance.

Car c'est bien sur une forte collaboration assureur - assuré que repose le succès : face à un risque émergent, l'information manque, et les deux parties ont besoin d'échanger celle-ci afin d'apprendre et de construire une protection, pas uniquement financière. Il faut ainsi rappeler le rôle historique de l'assurance face à d'autres périls : le risque incendie est souvent cité, où l'éclosion d'une vision collective, via l'assurance, a fortement contribué à développer et à diffuser des normes. De par le caractère évolutif de la menace, éteindre le feu du cyber est sans doute plus complexe. Mais pour aider à sa maîtrise, les innovations assurantielles et financières sont particulièrement prometteuses. ■

(1) McAfee and Center for Strategic and International Studies, *The Hidden Costs of Cybercrime*, (2020)

(2) AMRAE, LUCY : *Lumière sur la CYberassurance*, (2022)

(3) Hillairet C., Lopez O. *Propagation of cyber incidents in an insurance portfolio: counting processes combined with compartmental epidemiological models*, Scandinavian Actuarial Journal, 2021(8), 671-694

(4) Hillairet C., Lopez O., d'Oultremont L., Spoorenberg B. *Cyber-contagion model with network structure applied to insurance*, Insurance: Mathematics and Economics 107 (2022) 88-101