Assurer, réassurer et titriser les cyber-risques

Alexandre Hassler

Actuaire certifié, courtier en assurance et réassurance, Lyon Re

*Toujours plus spectaculaires et plus coûteuses, les cyberattaques ont gagné en médiatisation au fur et à mesure que la technologie a envahi le quotidien des entreprises et des consommateurs. Face aux cyber-risques, et plus que la cybersécurité, c'est désormais la cyber-résilience que recherchent les organisations du monde entier. À l'heure du bouleversement numérique, assureurs, réassureurs, courtiers, investisseurs d'*insurance-linked securities *(ILS) et tout l'écosystème assurantiel se mobilisent pour apporter une réponse durable à un enjeu sociétal d'avenir.*

Quel individu, quelle entreprise, quel État peut encore nier la réalité des cyber-risques ? Citées parmi les premières préoccupations des dirigeants économiques et politiques de tous les pays, les cyberattaques ont généré en l'espace de quelques années des pertes financières record qu'aucun expert n'aurait imaginé. Convaincus qu'il est impossible de garantir la sécurité totale de systèmes d'information de plus en plus complexes et interconnectés, ces mêmes dirigeants ont vu en l'assurance une réponse financière complémentaire aux efforts techniques de cybersécurité. C'est ainsi qu'est née la cyberassurance, un moyen de financement global des importants coûts consécutifs à un incident d'origine cyber : restauration de système d'information, reconstitution de données, remise en route de l'outil de production, prise en charge des pertes d'exploitation, devoir de notification... Sans oublier les mises en cause juridiques par les tiers : clients, fournisseurs, partenaires, autorités administratives.

Face à ces agressions numériques aux motivations économiques, hacktivistes, politiques et géopolitiques, le marché américain a ainsi été le premier à imaginer des couvertures contre les cyber-risques, surtout à destination des entreprises. Les assureurs en ont vite repéré le potentiel : un vecteur inexploité de différenciation à haute valeur ajoutée sur un risque d'actualité et un excellent relais de diversification sur un marché traditionnel très concurrentiel où les marges s'affaiblissent d'année en année. Ces cyberassurances se sont ensuite massivement développées avec l'apparition des réglementations relatives à la protection des données, notamment en Californie, alors qu'en même temps, les questions de cyber-résilience sont rapidement devenues des défis de sécurité économique puis des enjeux de sécurité nationale face à l'industrialisation du cybercrime via le Dark Net. Avec des montants de dommages et responsabilités absolument stratosphériques et de nombreux licenciements de dirigeants d'entreprise à leurs actifs, vers, virus, *ransomware, spyware* et autres DDoS ont alors pu s'inviter dans les

discussions de nombreux conseils d'administration et obtenir une place de choix sur la table des plus grandes directions financières, y compris dans des rapports à destination des actionnaires et autorités boursières pour lutter contre d'éventuels délits d'initié.

Beaucoup d'épineuses questions restées encore sans réponse détermineront dans quel avenir vivront nos sociétés : changement climatique, vieillissement des populations, transitions démographiques, bioéthique, émergence de totalitarismes démocratiques, géopolitique des zones polaires, raréfaction des ressources vitales et énergétiques, exploration et militarisation spatiales... Et les cyber-risques, avec le développement extrêmement impressionnant de la robotique et de l'informatique quantique, en feront évidemment partie.

Concilier cyber-risques, cyberassurance et prévention

Malgré l'arrivée du règlement général sur la protection des données (RGPD) et totalement sous-assurés en nombre et en montants, les plus gros acteurs économiques sont encore rares à avoir structuré une véritable stratégie de gestion des cyber-risques, à travers par exemple l'établissement d'une gouvernance cyber forte, la définition d'un cyber *risk appetite* ou encore la mesure quantitative de l'impact d'un programme de prévention ou de cyberassurance.

Pour la plupart des entreprises – rappelons que 99,8 % des sociétés françaises appartiennent à la catégorie des TPE-PME – dépourvues de tout rempart contre les agressions numériques, la cyberassurance n'est pas encore apparue comme une solution naturelle face à ces nouvelles menaces. Trop longs, trop techniques et trop intrusifs, les formulaires de souscription d'assurance cyber peinent à intéresser les assurés. Ils se demandent comment ils pourraient souscrire certaines assurances leur imposant de coûteux audits informatiques périodiques, des certifications spécifiques ou d'inquiétants logiciels de surveillance. Devant cette complexité pratique et avec un budget limité, ils préfèrent s'exposer à un risque conséquent et en pleine croissance que de payer annuellement une assurance cyber trop contraignante, même si beaucoup sont conscients de leur besoin. L'équation économique de la cyberassurance est donc très difficile à tenir dans ce contexte et nécessite d'en revoir les fondements : mener à bien l'appréciation des cybers-risques, suivre leur évolution dans le temps et anticiper les erreurs de déclaration non intentionnelles d'assurés perdus dans les méandres du jargon technologique.

Aujourd'hui, avec l'avènement de l'informatique de masse, les systèmes et les données évoluent quasiment en temps réel, les développements d'applications se font de manière agile, les infrastructures reposent sur des technologies *cloud* et l'IT peut être totalement externalisé. Le rapport des entreprises aux systèmes d'information, leur manière de les utiliser et de concevoir des logiciels a donc radicalement changé. Devant l'hétérogénéité des pratiques, le rôle du courtier en cyberassurance est d'appréhender la manière dont sont utilisés les systèmes et traitées les données chez le client pour évaluer dans quelle mesure une cyberattaque peut l'affecter opérationnellement et économiquement, établir quel type de coût et sous quelle amplitude son bilan et son compte de résultat vont être affectés, et ainsi formuler puis tarifer des garanties d'assurance en conséquence. Seule une approche sur-mesure pour un phénomène aussi évolutif et polymorphe que sont les cyberattaques permet donc de capter la profondeur des problématiques de l'assuré et de convertir un besoin de cyber-résilience en une transaction de cyberassurance.

Disposant d'un accès direct et privilégié avec l'assuré, il est ensuite aussi du ressort du courtier en cyberassurance de réanalyser périodiquement l'évolution des facteurs de risque et de détecter d'éventuels changements flagrants de comportement dans la prévention des cyberattaques ou dans la manière d'utiliser les outils technologiques ; car la souscription annuelle d'une cyberassurance fait l'objet d'un aléa

moral et d'un arbitrage important avec l'achat d'une prestation de sécurisation informatique amortissable sur plusieurs années. Sensibilisation périodique du personnel, lutte continue contre le *Shadow IT*, suivi intensif de la politique *bring-your-own-device* (BYOD), contrôle systématique des connexions inhabituelles, sécurité physique des infrastructures : tous ces efforts longs et coûteux sont autant de lourds investissements supplémentaires qui pourraient inciter les entreprises à réduire leurs actions de prévention à la suite de l'achat d'une police de cyberassurance. Le prix de cet aléa moral et le coût d'opportunité de cet arbitrage comptent ainsi pour une part non négligeable d'une prime de cyberassurance ; phénomène que doit anticiper le courtier dans son évaluation du risque et retraduire dans la structuration de la couverture.

Le passage d'un marché de niche disparate à un marché de masse efficient est essentiellement déterminé par la trajectoire qu'emprunteront distributeurs, assureurs et autorités prudentielles. Inciter à la prévention, contrôler l'aléa moral, réduire l'asymétrie d'information dont souffre l'assuré – via les faux produits estampillés « cyber » notamment – et trouver le juste équilibre entre réelle aversion au risque et incitation légale d'assurance cyber sont de sérieuses pistes pour favoriser naturellement la protection du tissu économique contre un risque nouveau et complexe.

L'assurance cyber : entre contrats dédiés et garanties silencieuses

Pénétrer efficacement le marché assurantiel des cyber-risques, c'est aussi en conserver une maîtrise suffisante sur le long terme. À côté de la prévention, cela passe aussi par l'identification claire et la quantification précise des expositions cyber dans les portefeuilles des sociétés d'assurance. On pourrait facilement penser que cela concerne exclusivement les contrats dédiés de cyberassurance. En réalité, il n'en est rien. Les garanties cyber se retrouvent aussi sous une forme implicite, silencieuse (1), dans les produits d'assurance traditionnels qui ne citent pas explicitement le cyber dans leur liste d'exclusions. Par conséquent, les expositions cyber sont extrêmement nombreuses dans les portefeuilles des sociétés d'assurance car tacitement incluses dans les contrats « tous risques sauf » vendus aux entreprises (contrats responsabilité civile, pertes d'exploitation, protection des mandataires sociaux, dommages aux biens, aviation, marine...) et aux particuliers (multi-risques, protection juridique...).

Ces garanties agissent comme une tumeur persistante contaminant l'ensemble des lignes de produits pour des milliers de milliards d'euros d'exposition. Parfois avec des centaines de millions d'euros à la clé, elles font l'objet de litiges entre assurés et assureurs portant sur la prise en charge d'un sinistre d'origine cyber et l'interprétation des contrats d'assurance traditionnels ne stipulant pas expressément l'exclusion cyber. Cette interprétation diffère évidemment d'un juge à un autre, d'un contrat à un autre, d'un assureur à un autre.

C'est d'abord dans l'intérêt de l'assuré d'apporter une réponse claire et transparente à la problématique des garanties cyber silencieuses... et d'un réseau de distribution, agents généraux et courtiers, qui n'est pas vraiment séduit par la perspective d'être mis en faute au titre de son devoir de conseil sacralisé depuis la directive sur la distribution d'assurance (DDA). Cette réponse appelle à passer en revue l'ensemble des produits d'assurance existants puis à identifier, qualifier et quantifier les garanties silencieuses cyber. À l'issue de ce travail minutieux, la société d'assurance a la possibilité d'éliminer une à une les garanties implicites résiduelles, quitte à éventuellement les inclure dans un contrat d'assurance cyber dédié, à les formuler en tant qu'option, ou à les laisser exister telles quelles dans ses produits en connaissance de cause. Une communication claire viendra alors informer l'assuré sur la prise en charge ou non d'un potentiel sinistre d'origine cyber à la vue de son contrat actuel, suivie éventuellement d'un ajustement tarifaire des contrats

d'assurance avec d'une part, la tarification du produit traditionnel et d'autre part, la tarification de la garantie implicite cyber ; voire d'une mise en *run-off* pour les produits les plus toxiques ou même la mise en place d'une commutation, sans oublier bien sûr l'instauration de systèmes d'information cohérents avec la stratégie choisie, tant au niveau de la souscription, de la tarification que de la gestion des sinistres ou des processus actuariels. Une démarche similaire s'applique dans le cas des traités de réassurance, à aligner sur la stratégie de souscription de la cédante. En résumé, un problème simple sur le principe, mais un chantier titanesque en pratique impliquant l'ensemble des métiers, des ressources et des partenaires des sociétés d'assurance jusqu'à leur gouvernance.

Gouvernance et solvabilité : un agrément pour émettre de la cyberassurance ?

Laisser les garanties cyber implicites infecter l'ensemble d'une ligne de produits d'assurance, c'est effectuer un bien dangereux pari sur la rentabilité et la solvabilité d'une société d'assurance : cela met en péril les actionnaires, les créanciers, les assurés et tout l'environnement économique. À tel point que, devant une telle crise prudentielle et une catastrophe systémique annoncée, le régulateur d'outre-Manche a préféré prendre les devants.

En l'espace de quelques années à peine, en incitant largement assureurs et réassureurs à identifier systématiquement les garanties cyber implicites de leur portefeuille, à les circonscrire et à leur donner une valeur actuarielle, les autorités prudentielles britanniques se sont assurées non seulement que l'impact des *cyber silent covers* était bien maîtrisé par les professionnels de l'assurance mais surtout, elles se sont aussi protégées contre un potentiel afflux de litiges complexes entre assurés, assureurs et réassureurs sur lesquels elles auraient de toute façon été amenées à trancher.

Solvabilité II n'a sans doute pas voulu insister sur les problématiques des assurances cyber-risques (implicites ou explicites) alors que la directive annonçait déjà par ailleurs d'importants changements pour le marché de l'assurance. Ces réflexions et ces inquiétudes nous invitent ainsi à imaginer dans quel contexte prudentiel la cyberassurance doit se développer. Il est évident que le cyber-risque revêt un fort caractère catastrophique : un piratage massif de données ou la cyberdestruction de systèmes industriels peuvent avoir des répercussions économiques, financières, sociales et politiques durables pour des millions d'individus, de petites entreprises, de grandes institutions ou de collectivités territoriales. Mais à la différence de la plupart des risques catastrophes, le fait que des institutions internationales de renom aient mis des années à détecter des cyberattaques nous invite à qualifier la cyberassurance de branche longue, avec les implications actuarielles que cela suppose en matière de tarification, de gestion des sinistres cyber, de *cyber risk management*, de provisionnement ou encore de modélisation actuarielle des cyber-risques. Cette hypothèse est corroborée par la crainte d'un important biais dans le nombre et l'amplitude des sinistres effectivement déclarés à un instant donné, notamment sur le marché des TPE-PME ; biais statistique dont la moyenne et la variance se réduiront si les évolutions technologiques permettent à l'avenir de détecter les incidents cyber plus efficacement et plus rapidement.

Pour toutes ces raisons, plusieurs dirigeants expérimentés de l'assurance et de la réassurance en viennent même à distinguer le cyber comme une catégorie complètement à part à côté des bien connus *Property* et *Casualty*. De là à considérer que l'émission d'assurance cyber-risques doit faire l'objet d'un agrément administratif préalable auprès des autorités prudentielles, il n'y a qu'un pas. Pas qui peut être aisément franchi en considérant que le modèle économique de la cyberassurance est bien différent des lignes existantes : mutualisation géographique clairement moins évidente, grande corrélation avec les autres lignes de produits du fait des couvertures cyber implicites, très grande asymétrie d'information à la

souscription et à la gestion des sinistres et, fait rarissime, risque très évolutif combinant fréquence et sévérité ! La stratégie d'optimisation de capital d'une société émettant du cyber n'est donc pas du tout la même que pour ses contrats traditionnels. A fortiori, la solvabilité d'une branche cyber ne peut être calculée de la même façon que les lignes existantes et le seul sinistre annuel bicentenaire n'est sans doute pas un indicateur pertinent pour apprécier un risque qui se métamorphose extrêmement rapidement au fil de l'évolution technologique. Ces éléments seront très certainement dans la tête de tous les professionnels de l'assurance, dirigeants, administrateurs et autorités de contrôle, qui voudront faire de la cyberassurance un marché de long terme, utile pour l'assuré et viable pour les porteurs de risques.

Cyber réassurance et captives cyber : des outils d'optimisation de capital

À l'heure d'une période de taux d'intérêt bas chronique, les stratégies d'optimisation de capital ne peuvent faire l'impasse sur les cyber-risques, qu'ils soient silencieux ou explicites. Plusieurs options permettant de combiner précision technique, justesse actuarielle et équilibre du capital s'offrent à tous les acteurs de la chaîne de valeur.

Du côté des entreprises, et pour les plus grandes d'entre elles, elles peuvent avoir recours à des transferts alternatifs de risques, notamment via la structuration de captives dédiées au cyber-risque, ou via son intégration dans leurs entités existantes, rentabilisant par là-même des coûts de fonctionnement importants. En s'exposant moins à un retournement de marché de la cyberassurance, les captives cyber permettent de modérer des hausses tarifaires que les assureurs devront de toute façon répercuter sur les grandes entreprises compte tenu des montants des sinistres cyber à payer et de la fin d'une logique de conquête de marché sur ce segment. Surtout, celles-ci s'assurent de disposer de réserves suffisantes, notamment avec des provisions d'égalisation autorisées dans certaines juridictions, dans le but de financer des expertises onéreuses d'identification des sinistres cyber, et de déceler d'éventuels faux positifs ou faux négatifs. Car rappelons-le, avant toute hypothétique prise en charge par un assureur, identifier l'occurrence et l'étendue d'un sinistre cyber est un processus long, complexe, coûteux et incertain.

Du côté des porteurs de risques, le choix des sociétés d'assurance pour se lancer sur le marché cyber a souvent été de se réassurer de manière proportionnelle, avec des taux de cession pouvant être extrêmement importants (jusqu'à 95 %), soit avec leur propre produit, soit en agissant comme distributeur d'une assurance cyber-risques en marque blanche conçue par des réassureurs. La réassurance cyber en quote-part est intéressante en première approche car elle permet un apprentissage du risque ; mais elle n'est pas optimale en matière de protection contre les risques extrêmes et de profitabilité au sens large. Car avec des ratios combinés cyber souvent très bas, le profil de rentabilité des produits cyber est plus proche des risques de type catastrophe que des risques traditionnels. C'est pourquoi les cédantes sont de plus en plus nombreuses à s'interroger sur la pertinence de disposer d'une stratégie de réassurance cyber plus structurée, plus modulable, via des couvertures annuelles agrégées, indicielles ou par événement, pour s'assurer à la fois un rendement du capital suffisant et une protection de réassurance cyber plus cohérente avec leur appétence au risque cyber.

Modéliser les cyber-risques et leur mutualisation

Face à ces nouveaux enjeux, de nombreux acteurs ont émis une inquiétude quant à la modélisation de leurs expositions cyber explicites et implicites, y compris les phénomènes d'accumulation cyber. Aujourd'hui pourtant,

de nombreux acteurs économiques – y compris Lyon Re – proposent des solutions de modélisation probabiliste des cyber-risques pour simuler et analyser les conséquences opérationnelles et financières d'une cyberattaque, notamment grâce au *big data*, avec une valeur ajoutée semblable à ce que l'on retrouve dans la traditionnelle modélisation catastrophe. Trois précautions sont sans doute à prendre.

D'abord, le fait que la sinistralité cyber anglo-saxonne est deux à trois fois plus élevée que la sinistralité cyber française impose de s'assurer au préalable que la modélisation effectuée est cohérente avec le portefeuille étudié, au risque d'entraîner une dérive très élevée, notamment pour les niveaux de probabilité les plus extrêmes. Ensuite, l'analyse des expositions cyber silencieuses est beaucoup moins automatisable et systématique que ne l'est l'analyse quantitative des expositions cyber explicites, et requiert un important travail manuel en amont que des logiciels, aussi complexes soient-ils, ne sont pas en mesure de réaliser efficacement.

Enfin, et davantage encore que la modélisation catastrophe traditionnelle, l'analyse technique ne sera pertinente que si elle revêt un caractère prospectif : à quoi bon en effet évaluer statiquement un portefeuille cyber dont le risque se modifie radicalement mois après mois ? Il implique ainsi pour les compagnies, d'une part, d'être en mesure de quantifier la sensibilité de leur portefeuille dans le temps au profil de leurs assurés et au profil de leurs contrats (garanties émises, montants accordés...) puis d'autre part, de projeter prospectivement l'impact des changements technologiques sur la rentabilité de leur ligne de produits ; et ils sont nombreux. À ce titre, si l'on s'intéresse par exemple à la manière dont réagit une *blockchain* à la suite d'une cyberattaque par rapport à un système traditionnel, il en ressort des conclusions absolument fascinantes qui peuvent être intégrées dans la modélisation d'un portefeuille cyber et aider les actuaires à mieux comprendre l'impact quantitatif de cette technologie sur le niveau et la mutualisation du cyber-risque au sein d'un groupe d'assurés à court et long terme.

Des *cyber bonds* face à des capacités limitées et peu liquides

Les cyber-risques d'aujourd'hui ne sont donc pas les cyber-risques des trois, cinq et dix prochaines années. Ces considérations importantes dans la stratégie de souscription, de gestion des risques et de réassurance nous posent ouvertement la question de la capacité assurantielle et réassurantielle que le marché est en mesure d'apporter à terme. La viabilité d'un marché d'assurance réside effectivement dans son aptitude à fournir des capacités suffisantes et liquides, y compris en cas de retournement ou de sinistre majeur. Aujourd'hui, à la vue des montants de sinistres cyber mis en jeu, cette condition n'est sans doute pas validée, même si des structures de type pool d'assurance ou de réassurance cyber, à la manière de ce qui existe pour le nucléaire ou le terrorisme, viendraient à émerger.

La complémentarité des ILS avec les stratégies traditionnelles n'est plus à démontrer. En exploitant les capitaux disponibles sur les marchés financiers, ils permettent en effet d'apporter une source de capital diversifiée additionnelle pour des opérations de rétrocession, de réassurance ou d'assurance. Dans la lignée des obligations catastrophes apparues dans les années 1990 – plus connues sous le nom de *catastrophic bonds* ou *cat bonds* –, une obligation catastrophe indexée sur le risque cyber permet d'indemniser le sponsor en cas de cyberattaque d'ampleur. Ces *cyber cat bonds* ou *cyber bonds* peuvent être émis par les sociétés d'assurance ou de réassurance souhaitant titriser une partie de leur portefeuille cyber auprès d'investisseurs et de fonds dédiés. Et il est aussi possible de le concevoir pour les grandes entreprises, les industries internationales, voire des États souhaitant trouver une source alternative de financement contre les cyber-risques grâce aux marchés financiers.

D'autres ILS cyber peuvent être structurés pour augmenter les capacités disponibles et la liquidité

du marché. Les véhicules de type *sidecars*, assez largement utilisés sur le marché de la rétrocession, constituent un complément intéressant à moindre coût et adaptable aux spécificités des cyber-risques. Des contrats financiers de réassurance de type *swap cyber* permettent quant à eux de se protéger des incertitudes à court ou long terme sur sa sinistralité cyber. Ou encore, les bien connus *industry loss warranties* (ILW), offrant des protections indicielles combinées basées sur les pertes de marché avec des coûts de mise en place réduits, sont tout à fait pertinents dans le cadre du cyber-risque du fait de son caractère naturellement systémique, et du fait d'une liquidité importante de ces instruments jusqu'à la détermination effective du montant des pertes à la suite d'une cyberattaque (2).

La structuration d'un ILS cyber suppose cependant de reconsidérer une hypothèse trop vite appliquée pour les ILS catastrophes traditionnels : celle d'indépendance entre le risque sous-jacent (tempête, séisme) et l'évolution des marchés financiers (cours des actions, obligations, devises). Bien qu'elle ne soit déjà pas totalement vérifiée en pratique pour ces ILS, dans le cas du cyber, l'expérience empirique montre aussi qu'une cyberattaque a un impact non négligeable sur le cours de l'action de la victime. Ce constat peut inciter l'assuré à émettre des instruments de type *cyber catastrophic equity puts* (*cyber CatEPuts*), car ils lui donnent le droit en cas de cyberattaque d'émettre des actions nouvelles à un prix fixé, permettant ainsi une recapitalisation à des conditions avantageuses pour se relever d'une cyberattaque qui mettrait grandement à mal sa solidité financière.

Ainsi, face aux cyber-risques, les solutions d'assurance, de réassurance et de titrisation sont abondantes et permettent de répondre aux importants besoins de financement des coûts consécutifs à une cyberattaque. Bien sûr, certains de ces mécanismes sont plus complexes à piloter et le cyber-risque requiert une réelle expertise assurantielle, mais aucun obstacle technique ou actuariel n'empêche désormais de les mettre en œuvre. Dans une période de métamorphose technologique extrêmement rapide, *blockchain*, intelligence artificielle, Internet des objets (*Internet of things* – IoT), voitures connectées, robotisation, G5, *fast data, edge computing*, impression 3D, informatique quantique ou encore industrie 4.0 sont autant d'éléments qui nous pressent de façonner un marché de la cyberassurance sain pour les assurés et durables pour l'industrie de l'assurance.

Remerciements : l'opinion exprimée dans ce dossier n'engage que son auteur. Pour avoir accepté de confronter leurs points de vue pendant l'écriture de l'article, il remercie chaleureusement :
- Jean-Louis Charluteau, *directeur de la réassurance de Generali France* ;
- Guy-Antoine de La Rochefoucauld, *directeur général du Lloyd's pour la France* ;
- Cyrille de Montgolfier, *cofondateur de Nemrod Finance* ;
- Emilie Desormeaux, *souscripteur et directrice de clientèle chez Swiss Re* ;
- Walter Eraud, *directeur général de Swiss Re pour la France, la Belgique et le Luxembourg* ;
- David Gierski, *directeur dommages de Gras Savoye Willis Towers Watson pour la France* ;
- Christophe Hassler, *agent général AXA et courtier d'assurance* ;
- Dominique Laure, *directeur général adjoint de Liberty Mutual Re* ;
- Laurent Montador, *directeur général délégué de CCR Re* ;
- Jean-Marie Nessi, *actuaire agrégé, ancien président-directeur général d'AXA Corporate Solutions* ;
- Luc Vignancour, *souscripteur international cyber chez Beazley.*

Notes

1. Littéralement traduit de « silent covers *» par opposition aux «* affirmative covers *».*

2. Voir à cet effet le marché de trading des ILW dits live cat *et* dead cat.