Le cyber en assurance, un risque presque comme les autres ?

Par **Benjamin DUCOS**
et **Luc de LIGNIÈRES**
AXA

Depuis plusieurs semestres, la forte croissance du nombre d'attaques cyber et la violence des conséquences extrêmes – opérationnelles, financières ou réputationnelles – qu'elles font peser sur les organisations qui en sont victimes renforcent la nécessité pour ces entreprises ou institutions de se protéger efficacement. Dans un marché de la cyber assurance estimé à moins de cinq milliards d'euros, mais en forte croissance – on parle de 30 % par an –, les regards se tournent vers les assureurs avec une double question : en quoi l'assureur peut-il contribuer, *via* des mécanismes d'assurance cyber, à la protection de ses clients, particuliers ou entreprises ? Et comment l'assureur se prémunit-il du risque opérationnel, c'est-à-dire du risque de ne pas être en mesure de servir ses assurés, face à la menace cyber ?

Le cyber en assurance, un risque presque comme les autres ?

Le risque cyber en assurance présente des caractéristiques d'un risque traditionnel en assurances dommages : il est incertain et imprévisible ; il se couvre en assurances tant pour les particuliers que pour les entreprises ; sa couverture d'assurance se définit à travers différentes garanties ; il peut toucher un ou plusieurs assurés simultanément comme cela arrive dans tout autre événement ; enfin, à l'instar de tout risque traditionnel, la prévention joue un rôle déterminant.

Pourtant le risque cyber présente des caractéristiques qui lui sont propres. Tout d'abord, il est systémique : comme un tremblement de terre, sa propagation peut être fulgurante, et toucher simultanément toutes les catégories d'assurés, qu'ils soient particuliers ou entreprises. Mais à la différence du tremblement de terre, il est potentiellement géographiquement sans limites. Il est également mal connu. La distribution du risque cyber s'apparente à une courbe qui tend vers un « Dirac [1] » : au regard d'événements moyens d'impact modéré, l'événement majeur est supposé très rare et ses conséquences extrêmes. Or, aucun événement majeur n'est survenu jusqu'à présent qui permettrait d'en déduire des impacts ! Le coût de l'événement majeur est donc soumis aux interprétations et estimations des parties prenantes dans la modélisation du risque (assureurs, fournisseurs de modèles, intervenants informatiques…). Dès lors, les primes d'assurance ne reflètent qu'imparfaitement le risque. Tant que l'événement majeur ne survient pas, la modélisation de la profitabilité du segment cyber reste incertaine. Enfin, il est en permanente évolution, sujet aux progrès techniques apportés dans l'industrie informatique, que ces progrès viennent des opérateurs, des dispositifs de sécurité mis en place par les clients ou de l'ingéniosité des hackers.

L'assureur dispose d'une double perspective sur le risque cyber : la compagnie d'assurance est à la fois dans le fauteuil du conducteur, en tant qu'assureur expert de ce type de risque, mais également sur le siège du passager, en tant que société majeure dans le paysage économique, et

(1) La distribution de Dirac est une fonction qui prend une valeur infinie en 0 et 0 sur le reste de la distribution. Appliquée au cyber, cela reviendrait à dire que l'événement de probabilité (quasi) nulle prend une valeur extrême alors que les autres événements de la distribution ont un coût (quasi) nul.

donc potentiellement cible d'attaques cyber. La stratégie cyber d'un assureur s'articule autour de deux volets : être capable d'offrir des protections d'assurance à ses clients contre le risque cyber (l'assureur cyber) tout en se protégeant lui-même contre le risque opérationnel émanant du cyber. C'est ainsi que la gestion du risque de l'information, au sens du risque opérationnel porté par l'assureur, et les fonctions commerciales ou expertes (tarification ou mesure de l'exposition par exemple) travaillent très étroitement ensemble pour faire progresser la connaissance qualitative et quantitative de ce risque.

La connaissance qualitative résulte en effet à la fois de l'observation jour après jour des risques et menaces qui pèsent sur l'assureur, d'un dialogue resserré entre chaque échelon de l'environnement de contrôle ainsi que d'un enrichissement mutuel avec les typologies d'incidents qui affectent les assurés. Des passerelles sont régulièrement à tirer entre les événements, afin d'accroître la compréhension de ces phénomènes : il ne se passe pas une semaine sans qu'un incident ne déclenche une investigation technique sous l'angle cyber, soit chez l'assureur en propre, soit chez un de ses assurés. La mesure quantitative est également une dimension-clé car elle permet de connaître, et donc d'agir, sur le niveau d'acceptation du risque cyber. Pour cela, les assureurs doivent identifier leur exposition au risque cyber au travers de leur activité mondiale d'assurance, d'une part, et de leur risque opérationnel lié à l'information, d'autre part. Des travaux qui sont menés sur ces quantifications doit découler une compréhension fine et chiffrée de l'exposition globale de l'assureur au risque cyber.

En tant qu'institution financière de premier ordre qui subit des attaques et qui gère ses propres risques opérationnels, l'assureur est donc bien placé sur ce sujet : le fait d'être à la fois une cible et un grand acteur de la prévention et de la protection permet d'allouer à la compréhension des ressorts du risque cyber des moyens plus importants que ne peuvent le faire d'autres acteurs. Et cette connaissance intime peut être partagée avec l'expertise mise à la disposition des assurés en matière de risque cyber.

De la couverture implicite à la couverture explicite… deux cas de figure

Pour l'assureur comme pour l'assuré, deux cas de figure se présentent :

- soit le risque cyber est implicitement protégé dans les couvertures traditionnelles au travers des garanties dommages aux biens ou responsabilité civile. On parle alors de « couverture silencieuse » (*silent coverage* ou *non-affirmative coverage)*.
- soit des garanties sont délivrées explicitement et spécifiquement pour couvrir le risque cyber. Ces garanties sont regroupées sous le vocable de « couverture affirmative » (en anglais, *affirmative coverage)*. Les garanties se subdivisent en trois segments : pour les entreprises, les garanties dommages propres (qualifiées de *first party* en anglais) couvrent les pertes subies sur les biens de l'assuré : pertes de données, perte d'exploitation, rançon et extorsion… Toujours pour les entreprises, les garanties de responsabilité civile (*third party* en anglais) qui protègent l'assuré contre les dommages aux tiers qu'il pourrait générer, de façon similaire à l'offre des garanties responsabilité civile : fuite de données personnelles, erreurs et omissions liées à la réalisation du risque cyber. Pour les particuliers enfin, les garanties offertes sont relatives au vol d'identité, au vol des moyens de paiement, à un conflit avec un commerçant en ligne ou encore à des actions de e-réputation visant à restaurer l'image sur Internet.

Nous pourrions penser que les couvertures silencieuses suffisent à protéger l'assuré contre le risque cyber et que les couvertures affirmatives sont donc inutiles. Ce n'est pas le cas car la couverture affirmative apporte un vrai plus en termes de garanties. Pour illustrer la différence entre couverture silencieuse et couverture affirmative, prenons l'exemple d'une usine affectée par une attaque cyber,

par exemple provoquant le dérèglement d'un programme informatique. Imaginons que cette attaque conduise à l'incendie de l'usine : la couverture silencieuse agit car le feu est couvert en dommages aux biens ; la couverture affirmative couvrira quant à elle la perte de données consécutive à l'événement cyber. Supposons maintenant que l'usine ne brûle pas mais ne puisse plus fonctionner : la couverture silencieuse ne peut jouer car il n'y a pas de dommages matériels (incendie ou dommage matériel aux machines par exemple) et la perte d'exploitation consécutive à un dommage matériel ne peut donc s'appliquer. La garantie cyber de la couverture affirmative, outre l'indemnisation de la perte de données, agit également au titre de la garantie perte d'exploitation *first party*.

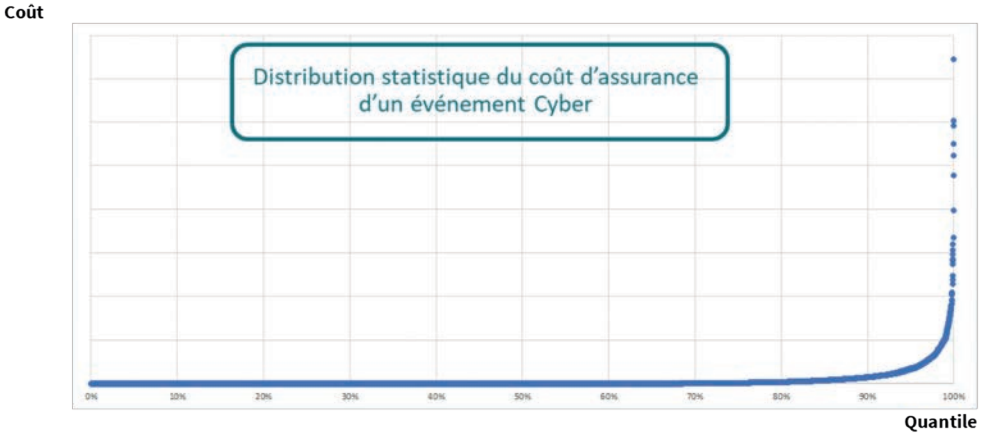
L'assurance cyber, poussée par les nouveaux usages

L'assurance cyber est le fruit de son époque, et son développement est le résultat combiné de plusieurs facteurs technologiques, réglementaires ou événementiels. Tout d'abord, l'utilisation massive de données et la digitalisation rapide des échanges avec les usagers ou les clients exposent les organisations aux risques de l'information (fuite, piratage, etc.) ; or, les nouveaux usages d'informatique dématérialisée et partagée (*cloud*) augmentent la surface d'attaque tout en l'étendant en dehors des frontières traditionnelles des organisations, par le truchement de l'externalisation. Concomitamment, ce sont les contraintes réglementaires et la judiciarisation croissante qui ont amené le marché américain de l'assurance cyber à prendre son essor avant le reste du monde. En effet, dès octobre 2011, la *Securities and Exchange Commission* (SEC) a imposé aux sociétés faisant appel à l'épargne publique de signaler sans délai les incidents de cybersécurité. Et de plus en plus, les législateurs, notamment européens, ainsi que les régulateurs du marché de l'assurance, incitent les opérateurs à se doter de mécanismes de cybersécurité robustes, ce qui les conduit à considérer l'assurance comme un levier essentiel parmi un ensemble de moyens de gérer ce risque : ainsi la directive européenne *Network and Information Security* de juillet 2016 (NIS, 2016/1148) engage les États membres à identifier les secteurs les plus critiques au fonctionnement de la Nation et à promouvoir la mise en œuvre de pratiques renforcées de cybersécurité chez les industriels désignés. D'autres règles ne sont peut-être pas étrangères à l'accélération de la demande de contrats d'assurance cyber : les nouvelles règles de protection des données personnelles (Personal Identifiable Information, PII) comme la norme PCI-DSS [(2)] et le RGPD [(3)], ont non seulement poussé les sociétés à investir pour se protéger et pour être en mesure de mener à bien leurs obligations déclaratives auprès des autorités, mais elles contribueront sans doute à les inciter à se couvrir avec des garanties assurancielles de plus en plus solides. Mais la nature internationale du risque cyber s'oppose à la logique réglementaire calquée sur des zones d'intervention géographiquement contenues. La nature des garanties elles-mêmes peut varier d'un pays à l'autre au gré de l'évolution de la maturité des marchés domestiques [(4)] ou en fonction des événements qui surviennent : la garantie « rançon », jusqu'alors peu mentionnée, s'est développée à la suite des deux grandes attaques par virus de 2017, *WannaCry* et *NotPetya*. Si la manifestation du risque cyber peut sembler évidente lorsqu'un assuré est sujet à une cyber-attaque soudaine et mondialement référencée (de type *Wannacry*), elle est plus délicate à circonscrire lorsque l'attaque est sournoise (logiciel malveillant), progressive dans le temps et que les connexions avec les dommages subis par l'entreprise sont difficiles à mettre en évidence. Cette difficulté est accentuée par la nature des garanties d'assurance mises en jeu, alors que la sinistralité passée, qui permettrait de s'appuyer sur un référentiel, est aujourd'hui rare voire absente, d'autant plus que le client lui-même n'est peut-être pas prêt à communiquer, par exemple, ses failles dans ses systèmes informatiques ou l'éventuelle demande de rançon dont il a été victime.

(2) *Payment Card Industry Data Security Standard*.
(3) Règlement Général sur la Protection des Données, entré en vigueur en mai 2018.
(4) N'oublions pas qu'entre les États-Unis, la France ou l'Espagne, le marché d'assurance évolue de 1 à 10.

Force est de constater que si les attaques cyber sont de plus en plus fréquentes et qu'il ne se passe pas une semaine sans qu'une entreprise ne fasse les frais de cette sophistication croissante de la menace, il n'y a pas encore eu à ce jour de « cyber ouragan » à grande échelle [5], au sens où plusieurs institutions ou organisations de plusieurs pays seraient massivement touchées, simultanément, par une ou plusieurs attaques, répondant à une même volonté. Dans un rapport de novembre 2018, l'Institut Montaigne a développé deux scénarios de cyber ouragan où, s'appuyant sur une quantification réalisée par les Lloyd's of London, les pertes mondiales coûteraient entre 4,6 milliards et 53,1 milliards de dollars (données 2017). On voit que ces scénarios sont très volatils et passent d'un extrême à un autre : l'incertitude domine encore. Dans ce contexte, c'est tout un marché qui se cherche, dans lequel l'assureur, par sa capacité à analyser les données existantes, à modéliser le risque à venir et à supporter le sinistre le cas échéant, est indéniablement un acteur-clé sur lequel s'appuyer.

Pour un assureur, l'évaluation du risque cyber passe en priorité par la connaissance de son exposition à ce risque ; sa capacité à associer pour chacune des garanties qu'il délivre l'engagement contractuel en montant est essentielle à l'appréhension du risque d'assurance cyber. En outre, comme pour tout produit d'assurance, c'est sur cet engagement que la prime d'assurance pourra être évaluée. L'assureur se doit donc d'être en mesure de connaître ce montant par garantie, par police d'assurance, par portefeuille d'assurance, par pays et monde entier. Cette mesure de l'exposition se fait spécifiquement par garantie dans le cadre des couvertures affirmatives. Elle se fait *via* le suivi des expositions aux garanties dommages aux biens et responsabilité civile traditionnelles dans les couvertures silencieuses. Enfin, comme le risque cyber est en évolution constante, la collecte de l'exposition doit être régulièrement mise à jour tant dans les montants alloués que dans la nature des garanties offertes. La sinistralité passée est l'autre élément à suivre en priorité. À partir d'un historique de sinistres qui s'enrichit au fil des ans à mesure que les garanties cyber s'étoffent et que le marché se développe, la vision du risque cyber est progressivement affinée. Toutefois, comme précédemment évoqué, la distribution des événements cyber tend vers une distribution « Dirac » :



Or, la prime d'assurance résulte avant tout de la moyenne théorique attendue de tous les sinistres qui peuvent potentiellement survenir. S'il y a peu d'expérience de sinistres connus, ce qui est le cas pour l'assurance cyber, la moyenne historique des sinistres apporte une contribution partielle à la

(5) Lire à ce sujet le rapport de novembre 2018 de l'Institut Montaigne « Cybermenace : avis de tempête, treize propositions pour augmenter la cyber-résilience de l'ensemble du tissu économique et de notre société » (2018) (https://www.institutmontaigne.org/publications/cybermenace-avis-de-tempete).

tarification. Et dans une courbe telle que ci-dessus, on comprend bien que l'événement extrême contribuera fortement à la moyenne théorique, et ce, beaucoup plus que pour des produits d'assurance traditionnels.

Par ailleurs, l'assureur doit être en mesure de mobiliser le capital suffisant pour absorber le coût de cet événement extrême, capital dont la rémunération est également à répercuter dans la prime d'assurance. On estime théoriquement que la rémunération du capital pour couvrir le risque cyber représente plus du tiers de la prime d'assurance alors qu'elle en représente en général moins de 10 % pour une branche d'assurances dommages. L'événement extrême, par son double impact dans la prime d'assurance, *via* sa contribution dans la moyenne théorique et *via* son impact direct dans la rémunération du capital, devient l'élément majeur de la fixation de la prime d'assurance. Négliger l'évaluation de l'événement extrême revient à sous-estimer de façon certaine la prime d'assurance associée au risque d'assurance cyber. Cela rappelle aussi l'importance du marché de la réassurance (l'assurance des assureurs) qui permet aux compagnies d'assurance de réduire le coût de cet événement extrême, soit en plafonnant son montant *via* des couvertures de sinistres appelées « en excédent de sinistres », soit en le partageant *via* des couvertures de réassurance en quote-part. D'autres couvertures, de type *Catbond*, peuvent également contribuer à réduire le risque d'assurance cyber. Dans ces montages, c'est le marché financier qui supporte le risque extrême s'il se déclare selon des conditions prédéterminées (un indice marché, un montant…) en échange d'une rémunération de type obligataire.

Une demande d'assurance en fort développement

Les entreprises qui souscrivent aujourd'hui des polices d'assurance cyber sont principalement les services financiers, les éditeurs de logiciels ou de solutions techniques, mais aussi l'hôtellerie et le commerce de détail, ainsi que les opérateurs de santé : tous cherchent à se prémunir contre les pertes d'exploitation qui résulteraient d'attaques cyber, et à se protéger contre les surcoûts engendrés par les conséquences de ces attaques, tant en conseil en communication de crise qu'en gestion du retour à la normale. Aux États-Unis ou au Royaume-Uni, une entreprise sur deux déclare ainsi avoir souscrit une assurance cyber. Si elles contribuent utilement à couvrir les risques des entreprises qui souscrivent leurs contrats, les compagnies d'assurance sont aussi prudentes, rappelle AM Best [6] dans une étude de juin 2019 : elles veillent à ce que leur exposition à ce risque ne dépasse ni leur appétit au risque, ni leur capacité financière. Même si le marché mondial de cyberassurance est estimé [7] à environ 5,3 milliards de dollars en 2018, il n'existe pas encore de chiffre agrégé de l'activité d'assurance cyber monde entier, soit du fait de la variété des régulateurs (EIOPA en Europe, NAIC aux États-Unis, OSFI au Canada, etc.), soit parce que tous les opérateurs et notamment les captives d'assurance ne sont pas tenus à des obligations similaires de reporting. Mais on observe un fort développement de la souscription de polices d'assurance et dans un marché qui croît d'environ 30 % par an, les analystes [8] estiment que le marché de cyberassurance pourrait encore doubler d'ici à 2020, et passer progressivement à environ 20 milliards de dollars d'ici à 2025. Le marché américain est le plus mature et le plus ancien : il a commencé à se développer dès le début des années 2000, et en 2017 il représentait 3,1 milliards de dollars de primes d'assurances [9] ; tandis qu'en France, le marché de la cyberassurance est relativement nouveau : il représente environ 80 millions d'euros à la fin 2018.

(6) https://www.insurancejournal.com/news/national/2019/06/18/529747.htm
(7) Etude PwC, *Insurance 2020 & beyond Reaping the dividends of cyber resilience* (2015).
(8) Etudes réalisées par PwC en 2015 (*Insurance 2020 & beyond Reaping the dividends of cyber resilience*) ou Munich Re en 2018 (*Cyber insurance market outlook*).
(9) Rapport, *National Association of Insurance Commissioners* (août 2018).

Le risque cyber pour l'assureur AXA : servir ses clients tout en se protégeant

Le risque cyber majeur auquel AXA peut être exposé n'est pas de même nature entre risque d'assurance et risque opérationnel. En effet, le hacker, source du risque majeur, a deux façons d'intervenir : soit il cherche à occasionner massivement des dégâts et à affecter le plus grand nombre (premier cas) ; soit il vise spécifiquement une entreprise, dont il aura étudié au préalable les failles technologiques, qu'il cherchera ensuite à affecter le plus sévèrement possible (second cas). À titre d'exemple, le rançongiciel *WannaCry* a utilisé en mai 2017 une faille de sécurité Windows, qui avait fait l'objet d'un correctif livré deux mois avant par l'éditeur [(10)] mais que de nombreuses compagnies n'avaient pas encore installé. Le virus a donc infecté un grand nombre d'ordinateurs parmi cette population vulnérable, générant de nombreuses pertes, mais sans cible particulière. À l'inverse, lorsque, en décembre 2013, un hacker attaque Target, la troisième enseigne américaine de supermarchés, c'est précisément cette société qui est visée avec peu d'impacts collatéraux sur d'autres assurés. Dans un scénario extrême, le risque d'assurance est maximal dans le premier cas car le montant assuré dépend du nombre de victimes, inconnu *a priori,* alors que dans le second cas, le sinistre ne peut pas dépasser la garantie contractuelle donnée à l'assuré visé. À l'inverse, le risque opérationnel sera maximal si AXA est ciblé par l'attaque d'un hacker (second cas), alors que les répercussions du premier cas resteront limitées car les protections demandées demeurent « standard », et bien moindres que celles exigées dans le deuxième cas.

Afin de suivre le risque assurance, AXA a donc développé un modèle dédié au cyber qui s'appuie sur plusieurs étapes. La première étape consiste à identifier et collecter les expositions d'assurance au risque cyber par police d'assurance au sein du groupe (nature des garanties et montants de couverture). Dans la deuxième étape, des scénarios existants ou potentiels sont modélisés « physiquement » de façon à appréhender notamment les enjeux maximums auxquels AXA est exposé. Enfin, la troisième étape aboutit à transposer statistiquement la vision par scénario de la deuxième étape et à permettre ainsi d'attribuer à des périodes de retour d'événements les coûts d'assurance induits. Chaque année, cette approche est affinée au gré des événements cyber nouvellement survenus, de l'expérience sinistres afférente, des améliorations internes de collecte de données et de modélisation.

On comprend bien que la seconde étape, la modélisation de scénarios, est primordiale pour mesurer à quel risque extrême s'expose AXA. Elle repose sur trois actions principales :

- La constitution et la mise à jour de la bibliothèque de scénarios : quels scénarios considère-t-on comme critiques pour AXA étant donné sa typologie de risques (catégories de clients, nature des garanties, montants de garanties alloués, etc.) ? À quels scénarios de marché se réfère-t-on ?
- Le développement du modèle « physique » : à l'image d'un processus industriel, en fonction du scénario retenu, AXA établit ses hypothèses de modélisation théorique : comment se propage l'événement cyber ? Qui est touché ? Quelle est l'ampleur de la destruction, qui dépend entre autres de la nature des clients affectés ? La réponse à ces questions et leur modélisation permettent d'estimer le coût maximal théorique auquel AXA pourrait être exposé.
- La confrontation des résultats à des experts – qu'ils proviennent du groupe AXA ou qu'ils soient issus du monde académique – ou la comparaison avec d'autres modèles développés sur le marché.

Dans ce contexte, les compétences demandées pour appréhender le risque assurance sont à la fois la connaissance assurancielle (connaissance de la mécanique d'assurance cyber et de la nature

(10) Bulletin de sécurité MS-17-010.

des garanties), la compréhension de la nature du risque (un événement affectant l'informatique dématérialisée et partagée (*cloud*) ou de type rançongiciel (*ransomware*) n'impacte pas le marché de la même manière), et la compétence actuarielle (collecte de données et approche stochastique). AXA développe en interne cette connaissance qui est enrichie par des recherches académiques, notamment *via* une Initiative de Recherche conjointe avec l'École nationale de la Statistique et de l'Administration économique (ENSAE) et Sorbonne Université. Par ailleurs, le fonds AXA pour la Recherche, en finançant des chaires dans ces domaines, contribue également à cet enjeu associant recherche interne et recherche académique.

Considéré maintenant en tant que risque opérationnel pour l'assureur lui-même, le cyber requiert à la fois une compétence affûtée en gestion des risques ainsi qu'une vaste connaissance des systèmes informatiques. La société d'assurance va modéliser des scénarios reposant sur différentes histoires vraisemblables où tout ou partie des systèmes d'information sont l'objet d'attaque, d'indisponibilité ou encore de corruption de données. Ces « histoires » sont analysées, disséquées, et associées à des unités de valeur (coût de personnel, coût de remédiation, perte d'exploitation, etc.) : elles permettent d'évaluer le coût réaliste d'un tel scénario. Les données proviennent de l'entreprise elle-même (parc de machine, configuration, etc.) ainsi que de son expérience réelle des incidents récents et, dans certains cas, de données provenant de sachants extérieurs à l'entreprise : cabinets de conseil, entreprises du marché ou encore associations professionnelles. Chez AXA, de tels scénarios sont réalisés annuellement et collectés à travers toutes les entités qui constituent le groupe : la somme de ces scénarios, ou leur corrélation, permet de calculer une charge en capital requise dans le cadre de Solvabilité II. Au-delà de l'obligation réglementaire, ces travaux permettent une quantification des impacts possibles d'événements majeurs et facilitent donc les discussions et la hiérarchisation des priorités quant aux moyens d'en empêcher la survenance ou d'en ralentir les effets. Cette quantification des risques cyber ne se fait pas en silo mais participe d'une organisation globale en lignes de défense complémentaires : si les opérationnels sont les premiers acteurs de la gestion de leurs risques, eux-mêmes appuyés par des experts de première ligne qui répondent à une stratégie décidée et suivie globalement par la direction de la sécurité du groupe, notamment en matière de cyberdéfense, des fonctions de seconde ligne sont positionnées dans chaque entité au sein du *risk management*. Celles-ci aident à anticiper les risques de l'information, en procédant à la modélisation des risques, mais aussi en questionnant les décisions à prendre, lors de comités stratégiques, afin d'obtenir la mise en œuvre d'un environnement de contrôle fiable ; ces experts du risque aident aussi à orienter l'allocation de moyens sur les bonnes priorités, et enfin organisent la restitution de ces sujets au comité des risques. Une gouvernance décisionnaire de haut niveau, le *Group Information Risk Board*, permet d'ailleurs d'engager le groupe dans des mesures préventives ou curatives, elles-mêmes régulièrement auditées dans un évident souci d'amélioration continue.

En conclusion

De façon générale, l'assurance d'un risque naît de sinistres qui génèrent des pertes économiques importantes et qui soulignent le besoin d'une protection d'assurance afin de permettre le maintien de l'activité professionnelle en toute circonstance assurée (client entreprise) ou de préserver le patrimoine privé (client particulier). L'assureur appuie alors son estimation du risque sur la base des pertes antérieures. De son côté, le risque opérationnel, au sens de la directive Solvabilité II de 2009, a un périmètre restreint à une entreprise et, à ce titre, la gestion du risque opérationnel s'intéresse à anticiper les risques extrêmes auxquels l'entreprise pourrait faire face, en s'appuyant à la marge seulement sur les événements du passé. Ces deux approches ne s'appliquent pas aussi facilement au risque cyber. Le risque cyber est nouveau en assurance et personne ne sait quantifier les pertes antérieures, nul ne saisit pleinement le risque d'autant plus qu'il évolue sans cesse – l'une des problématiques actuelles est par exemple l'imputabilité d'un acte de guerre réalisé au travers

d'un piratage informatique – mais tout le monde sait que le risque cyber est potentiellement majeur et justifie une protection d'assurance. Incité par les assurés demandeurs de protection, l'assureur doit prendre un risque qu'il ne connaît pas et dont il n'a pas pu mesurer les conséquences passées.

Le risque cyber est dorénavant inhérent à toute activité, qu'elle soit entrepreneuriale ou individuelle. L'assureur se doit donc d'accompagner son client dans son activité en lui apportant conseils en prévention et solutions de protection appropriées à ses besoins. Mais l'enjeu est aussi de permettre que l'assureur soit toujours en capacité de servir ses clients : qu'en temps ordinaire, il protège les données qui lui ont confiées et qu'en cas de sinistre, il assiste ses assurés. En effet, en cas de catastrophe naturelle, chacun s'attend légitimement à ce que son assureur soit debout ; il en va de même pour les événements cyber, où l'assureur doit pouvoir résister à un cyber ouragan : il lui faut donc anticiper le risque cyber en étant toujours à la pointe de la protection et en restant en permanence en veille. La menace cyber est ainsi faite : pour être en mesure de proposer à ses clients les garanties qu'ils demandent, un assureur doit viser un très haut niveau de protection opérationnelle. C'est un défi nouveau mais stimulant !