Cyberassurance : offres et solutions

Didier Parsoire

Responsable de souscription « cyber », SCOR Global P&C

Le monde est entré dans l'ère numérique. L'information devient vitale pour les entreprises. Internet démultiplie les échanges mais aussi les risques au sein du cyberespace. Les atteintes aux données et aux systèmes d'information (SI) se font plus sophistiquées et causent de plus grands dommages aux entreprises.

Face à ces risques, le marché de la cyberassurance, né il y a une quinzaine d'années, a véritablement pris son envol aux États-Unis vers la fin des années 2000 sous l'impulsion réglementaire. Le marché européen est, lui, encore naissant. L'offre de réassurance est balbutiante en raison du manque d'outils destinés à contrôler les accumulations de risques. Ce marché possède un fort potentiel de croissance dû aux enjeux qui occupent les entreprises et les gouvernements. Il lui faut néanmoins gagner en maturité sur toute la chaîne : de la gestion du risque par les entreprises à la mesure des expositions et des concentrations de risques par les assureurs et les réassureurs, en passant par la détermination du risque transférable au marché. Une véritable expertise doit se développer chez tous les acteurs pour en faire un marché pérenne.

Chaque année, la quantité des informations stockées sous forme numérique dépasse le volume du savoir humain qui nous est parvenu avant l'ère digitale. À la révolution industrielle succède la révolution numérique. L'information est la nouvelle matière première des agents économiques. Elle est collectée, transformée, stockée, échangée. Elle est le substrat d'une grande partie des produits et services que nous consommons. Dans cette nouvelle ère, l'ordinateur remplace la machine-outil ou en prend tout au moins le contrôle. Cette révolution des usages a été rendue possible par un développement exponentiel des technologies. La puissance de calcul et les capacités de stockage sont à la portée de tous, à moindre coût. Surtout, Internet et les infrastructures de communication ont permis, par la circulation planétaire de l'information, de décupler l'efficience des organisations et des processus.

La « cybernétique » a désigné, dès le milieu du XXe siècle, la science naissante de l'information et des automatismes. Aujourd'hui, nous en avons gardé l'abréviation « cyber », dérivée du mot grec *kubernan* signifiant « gouverner », que l'on décline à l'envi pour désigner les acteurs, les concepts et les objets de ce nouvel espace numérique.

Cyber-risques : un large éventail de menaces

Dès lors que l'information et son traitement innervent l'économie et les entreprises, le bon fonctionnement des systèmes informatiques est devenu capital. L'interconnexion offerte par les réseaux d'information a rendu de surcroît ces systèmes vulnérables aux attaques extérieures. Ainsi, le développement d'Internet a ajouté la menace intentionnelle au risque de nature accidentelle qui prévalait jusqu'aux années 1990.

Cette menace progresse et s'organise au fur et à mesure que l'information croît en volume et en valeur. Le « hacker » solitaire a fait place à la cybercriminalité, au cyberespionnage, au « hacktivisme » ou au cyberterrorisme, qu'ils soient le fait d'organisations ou d'États. Les motivations sont multiples : atteinte aux actifs tangibles ou intangibles de l'entreprise, intelligence économique ou géostratégique, gain financier… Les stratégies déployées (déni de service, défiguration de site Internet, logiciels malveillants, *phishing*, ou « hameçonnage », pour soutirer des informations, etc.) évoluent sans cesse et s'appuient sur des outils technologiques toujours plus sophistiqués et plus accessibles pour créer les vecteurs d'attaque. Surtout, les assauts les plus pernicieux révèlent un degré de préparation très élevé reposant sur une connaissance fine de l'objectif via l'ingénierie sociale, l'employé négligent ou indélicat.

D'une façon ou d'une autre, l'attaquant va exploiter certaines vulnérabilités identifiées de la cible. Là résident les cyber-risques. Et leur survenance peut mettre à mal l'entreprise non préparée : vol de millions de données de clients, divulgation de données sensibles de l'entreprise, demande de rançon (cyberextorsion), etc. Ces événements nécessitent une gestion de crise qui n'est pas sans rappeler celle engagée pour le rappel de produits défectueux ou en cas de demande de rançon à la suite du kidnapping d'employés ou de dirigeants.

C'est bien à ces nouveaux risques que tente de répondre le marché de la cyberassurance depuis l'avènement d'Internet, il y a plus d'une quinzaine d'années.

L'actualité récente, qu'il s'agisse des « mégafuites » de données survenues ces derniers mois ou des révélations de la mainmise des États sur nos données privées, oblige les différents acteurs de ce marché – assurés, courtiers, assureurs et réassureurs, mais aussi pouvoirs publics – à reconsidérer la nature du risque et les réponses qui peuvent être apportées.

Les différentes motivations d'achat de cyberassurance

La cyberassurance reste aujourd'hui un marché essentiellement nord-américain. Environ deux milliards de dollars de primes ont été collectés aux États-Unis en 2014, quand le marché européen en comptabilisait six fois moins. Encore faut-il s'entendre sur le décompte des primes : plus de la moitié de celles-ci proviennent de contrats combinant des garanties « cyber » et responsabilité civile (RC) professionnelle, en particulier pour les entreprises du secteur des TMT (technologies, médias, télécommunications). Ces deux marchés révèlent des dynamiques respectives très différentes.

Le catalyseur du développement de la demande aux États-Unis a été la mise en place par la plupart des États de réglementations visant à protéger les particuliers contre la violation de données à caractère personnel. Aujourd'hui, seuls trois États n'en sont pas encore dotés. Si les modalités diffèrent d'un État à l'autre, les entreprises sont dans l'obligation d'avertir les personnes concernées par les fuites de données, sous peine de sanctions. Par ailleurs, depuis 2011, la Securities and Exchange Commission (SEC) impose aux entreprises cotées de déclarer toute exposition significative aux cyber-risques et tout cyberincident majeur. Conjugué à l'importance des *class actions* (« actions de groupe »), cet environnement a conduit au développement de contrats « cyber » couvrant la

responsabilité des entreprises en cas de fuite de données (*data breach*) ainsi que les frais de notification aux tiers et de gestion de crise. Ce marché a vraiment pris son essor à la fin des années 2000.

En Europe, le cadre réglementaire actuel n'est pas le même. Il impose la notification de violations de données personnelles par les seuls opérateurs de communications électroniques (Internet, téléphonie) aux autorités nationales (la Cnil en France) et, dans certains cas, aux personnes concernées. Surtout, les sanctions financières sont bien moins lourdes qu'aux États-Unis. D'autre part, la possibilité (ou la culture) des actions de groupe est encore naissante. Dès lors, les entreprises se tournent en général plutôt vers la protection de leurs intérêts propres en mettant l'accent sur la couverture des incidents de sécurité de leur système d'information et de la perte d'exploitation qui en découle.

Des différences existent aussi entre l'Europe et les États-Unis relatives au niveau des limites d'assurance des contrats « cyber » spécifiques. Si elles peuvent atteindre 200 à 300 millions de dollars aux États-Unis, elles restent pour le moment inférieures à 150 millions d'euros en Europe. De même, le taux de pénétration des cyberproduits se distingue entre ces deux marchés. Il est assez difficile à établir précisément et dépend de la taille des entreprises, mais on estime qu'il se situe, selon les secteurs d'activité, entre 10 % et 50 % aux États-Unis, les institutions financières et le secteur de la santé en étant les principaux acheteurs. En Europe, le taux d'achat est bien moindre.

Les cyberassureurs : plusieurs générations d'acteurs

Le marché de la cyberassurance rassemble des acteurs de profils très différents : des assureurs généralistes, des assureurs spécialisés, des agences de souscription, des syndicats et consortiums du Lloyd's.

Quelques acteurs comme AIG, ACE ou Beazley ont été parmi les premiers du marché. Ils ont développé une offre internationale diversifiée combinant couverture d'assurance et assistance aux clients (évaluation des risques, gestion de crise). La plupart des autres acteurs ont émergé aux États-Unis et sur le marché de Londres lors des dix dernières années.

Plusieurs assureurs déclinent maintenant des produits pour l'Europe. Ces derniers mois, une nouvelle génération de « pools » et d'agences de souscription se positionne sur des produits ou des services nouveaux : protection des infrastructures industrielles, offre combinant assurance et service de détection d'incidents. Pour compléter le panorama, il faut aussi compter quelques réassureurs intervenant en facultative ou sur le marché direct. Au total, entre cinquante et soixante acteurs, présents aux États-Unis ou en Europe, interviennent sur le segment de l'assurance des grands comptes ou des PME.

Les capacités offertes varient de 5 millions de dollars à 100 millions de dollars et peuvent être supérieures pour certains pools. Le cœur de marché se situe probablement entre 10 millions de dollars et 15 millions de dollars, et, en pratique, peu d'acteurs ont réellement engagé à titre individuel plus de 25 millions de dollars à ce jour.

S'agissant plus spécifiquement du marché français, on recense actuellement onze acteurs d'assurance offrant une capacité théorique globale supérieure à 300 millions d'euros : ACE, AIG, Allianz, AXA Corporate Solutions, Beazley, CNA, Hiscox, Munich Re CIP, Swiss Re Corporate Solutions, XL, Zurich.

La cyber-réassurance en devenir

Jusqu'à récemment, les capacités engagées et la taille des portefeuilles « cyber » ne justifiaient pas l'appel à la réassurance. Cependant, la demande croît depuis quelques années. La cession des cyber-risques, quand elle a lieu, se

fait pour l'essentiel par extension des traités de RC professionnelle. On a vu aussi apparaître quelques traités de cyber-réassurance spécifiques principalement sur base proportionnelle pour accompagner le développement de cédantes sur ce segment. Le caractère mixte des contrats « cyber » (dommages et responsabilité) en rend la cession quelque peu difficile.

Aujourd'hui, la taille des portefeuilles et la gestion des cumuls de risques conduisent les assureurs à rechercher des protections de fréquence (*stop loss*) ou de type catastrophe. Les cybersinistres pouvant potentiellement impliquer des contrats traditionnels (dommages, RC professionnelle ou RC des mandataires sociaux, fraude, etc.) en sus des contrats spécifiques, on voit aussi apparaître des demandes de protection « clash » multilignes.

Il n'y a pas aujourd'hui de modélisation crédible ni de scénarios permettant la quantification des cumuls de cyber-risques. Par ailleurs, les critères spatiaux ou temporels habituels ne se révèlent pas pertinents pour définir un « cyberévénement », puisque Internet se joue des frontières et que les cyberattaques sont parfois découvertes plusieurs mois après avoir été perpétrées. Enfin, il est très rare de pouvoir remonter à la source de l'attaque. Un immense chantier s'ouvre donc sur l'évaluation et le contrôle des cumuls de risques. Le développement de l'offre de réassurance en dépend.

L'assurance des cyber-risques en quête de maturité

Un fort potentiel de demande...

Une conjonction de facteurs crée un fort potentiel de demande pour la cyberassurance.

Tout d'abord, les entreprises sont toujours plus dépendantes des technologies de l'information et, dans le même temps, éprouvent une difficulté grandissante à contrôler l'information. Externalisation des prestations informatiques, développement du *cloud*, traitement de plus en plus complexe de l'information, notamment via les approches « *big data* », nouveaux usages – réseaux sociaux, « *Bring your own device* » (Byod) – et relation au monde physique via les objets connectés, toutes ces tendances dispersent l'information, en démultiplient les canaux d'accès, amplifient les risques existants et en créent de nouveaux (dommages matériels ou corporels).

Parallèlement, les gouvernements expriment un intérêt croissant pour le cyberespace, devenu enjeu de guerre économique et politique. Les menaces terroristes sont le moteur (et parfois le prétexte) d'un contrôle croissant des échanges sur Internet. La protection des données personnelles se développe. Un règlement européen est en cours de discussion et pourrait s'avérer contraignant pour les entreprises en ce qui concerne la notification aux autorités en cas de violation de données personnelles. Les États-Unis réfléchissent à une harmonisation fédérale des multiples réglementations existantes en la matière.

La gouvernance des entreprises est aussi à l'ordre du jour tant les attaques récentes ont montré les risques qu'elles font porter sur leur existence même.

La préservation des infrastructures critiques (eau, énergie, services financiers, transports, etc.) fait l'objet d'une attention croissante de tous les États. En France, la loi de programmation militaire comporte des dispositions spécifiques en matière de cybersécurité s'appliquant aux opérateurs d'importance vitale (OIV).

Enfin, la série sans précédent des cyberattaques majeures survenues ces derniers mois révèle l'ampleur de la menace et suscite une sensibilisation accrue au risque : Target, JPMorgan Chase, Home Depot, Sony, Anthem, etc., soit des centaines de millions de données dérobées, des attaques sophistiquées et des motivations diverses (gain financier, atteinte à l'entreprise). L'actualité récente a montré l'asymétrie de moyens entre attaquants et défenseurs, et les difficultés, voire le manque de préparation, des

entreprises pour faire face à ces attaques. Les pertes potentielles sont considérables et peuvent facilement dépasser les limites actuelles de l'assurance, sans même parler des risques inassurables (perte d'image, par exemple).

... mais des défis à surmonter

Ce contexte offre des opportunités réelles au marché de l'assurance et de la réassurance. Pour autant, un grand nombre de défis doivent encore être surmontés.

En effet, les entreprises éprouvent encore des difficultés à gérer leurs risques et à évaluer leurs besoins d'assurance. La gestion du cyber-risque est encore trop fragmentée entre de multiples directions (informatique, risk management, juridique, etc.) et manque bien souvent d'une vision globale des actifs et processus à risque. L'apport des contrats « cyber » spécifiques par rapport aux contrats traditionnels n'est pas toujours clairement identifié par les acheteurs d'assurance, et des doublons de garantie peuvent exister.

De leur côté, les assureurs peinent à évaluer et à tarifer les risques. Il existe un manque de données historiques sur les sinistres et incidents, renforcé par la réticence des entreprises à partager l'information. D'autre part, l'évolution rapide des technologies et des profils de menace rend difficile l'extrapolation à partir de l'expérience passée. Une autre difficulté à laquelle se heurte l'évaluation de l'assureur est l'absence de référentiel ou de standard partagé par les entreprises en matière de gestion du risque.

Par ailleurs, l'identification des cumuls d'engagement et des scénarios catastrophes reste difficile. Des exemples récents l'illustrent : une cyberattaque peut potentiellement affecter plusieurs contrats d'assurance traditionnels (RC professionnelle, RC des mandataires sociaux, dommages, RC générale, etc.) en sus ou en l'absence de couvertures « cyber » spécifiques. De plus, les risques de sinistres sériels à grande échelle sont bien réels : interconnexion des systèmes et standardisation des produits informatiques créent un risque de propagation virale, et l'externalisation par le *cloud* génère des concentrations de risques chez les fournisseurs. Nous l'avons déjà évoqué, le marché manque aujourd'hui de données, de modèles et de scénarios pour évaluer ces cumuls.

En dernier lieu, on observe un manque d'expertise chez l'ensemble des acteurs concernés. La pénurie d'experts en cybersécurité est patente dans le tissu industriel en général. Elle est encore plus évidente chez les acheteurs d'assurance, les porteurs de risque et les intermédiaires. La science des cyber-risques n'a pas encore vraiment pénétré le marché de l'assurance.

Conclusion

On le voit, même si ce marché a maintenant une quinzaine d'années d'existence, la cyberassurance et plus généralement la gestion du cyber-risque doivent se réinventer à la lueur des changements intervenus dans le paysage des risques sous-jacents.

L'assurance et la réassurance ne peuvent assumer le risque d'entreprise ou se substituer à une gestion optimisée des risques, mais elles joueront pleinement leur rôle dans la chaîne de gestion et de portage du risque dans la mesure où l'information sera organisée et partagée entre les différents acteurs afin de permettre une meilleure évaluation des risques et un contrôle des cumuls d'engagement. Le marché sera alors à même de structurer les capacités nécessaires, de développer des solutions spécifiques et d'adapter ses offres en fonction des différents segments d'exposition. Les États devront aussi s'impliquer dans la couverture des événements majeurs de type cyberterrorisme ou cyberguerre, qui dépassent par leur ampleur les capacités du marché.

La prise de conscience généralisée qui s'observe actuellement doit servir de catalyseur pour que non seulement les acteurs de marché mais aussi les pouvoirs publics définissent le cadre et les moyens du développement d'un marché pérenne de la cyberassurance.