LA COUVERTURE DU CYBER-RISQUE

Extrait de la Revue d'Economie Financière n°126

Auteurs:
Sébastien HEON
Directeur Adjoint, Cyber Solutions, SCOR Global P&C
sheon@scor.com

Didier PARSOIRE
Directeur, Cyber Solutions, SCOR Global P&C
dparsoire@scor.com

2017

SCOR
The Art & Science of Risk

RÉSUMÉ :

La numérisation de l'économie, si elle est facteur de progrès, emmène son lot de nouveaux risques, cybercriminalité et autres formes d'attaques, qui viennent en éroder les bénéfices. Alors que l'arsenal d'outils et de services de sécurité informatique se développe pour contrer les attaques, les entreprises sont à la peine pour en quantifier les impacts. Dans un contexte économique et géopolitique favorable aux attaquants, les Etats prennent conscience des risques et se dotent de réglementations de plus en plus globales.
Le marché de la cyber-assurance est en construction et ses produits en phase d'ajustement. Alors qu'il jouit d'une croissance soutenue, il se heurte cependant à la méconnaissance d'un risque récent et évolutif et au potentiel de cyber-catastrophes qui freinent l'offre de réassurance. Gestion du risque par les assurés, environnement réglementaire adapté et développement de l'expertise chez les assureurs et réassureurs sont les conditions pour que ce marché parvienne à maturité.
Au-delà de sa seule couverture, le péril Cyber est révélateur des transformations à venir dans le paysage des risques pour le marché de l'assurance et de la réassurance.

ABSTRACT :

The digitization of the economy is a driver of progress, but it also brings its share of new risks, such as cybercrime and other forms of cyberattack, which eat away at profits. Despite the growing arsenal of IT security tools and services designed to counter such attacks, businesses are still struggling to quantify their impact. In an advantageous geopolitical and economic environment for attackers, States are becoming aware of the risks and are developing increasingly global regulations.The cyber-insurance market is under construction and its products are in a phase of adjustment. While it enjoys sustained growth, it is also confronted with the lack of knowledge surrounding this emerging and evolving risk, and with potential cyber-catastrophes, which is hindering the reinsurance offering. To reach maturity, this market needs sound risk management by the insured, a suitable regulatory environment and the development of expertise among insurers and reinsurers. Over and above coverage, the Cyber peril is indicative of the transformations to come in the insurance and reinsurance risk landscape.

LA COUVERTURE DU CYBER-RISQUE

LE NUMÉRIQUE TRANSFORME NOS SOCIÉTÉS ET NOTRE PAYSAGE DES RISQUES

La numérisation de l'économie se développe rapidement au point que la valeur des actifs intangibles des sociétés commence à dépasser la valeur de leurs actifs tangibles, comme le rapporte une étude menée par AON et Ponemon Institute publiée en avril 2017[1] et portant sur un panel de plus de 2 000 entreprises du monde entier. Ce changement de paradigme confirme l'analyse de l'OCDE (Organisation de coopération et de développement économiques) qui, dans un rapport de juin 2016 (OCDE, 2016), reconnaissait le lien entre la nature ouverte, distribuée et interconnectée d'Internet et son rôle de catalyseur pour la croissance économique et le bien-être social. Effectivement la numérisation et le développement foisonnant de nouvelles technologies favorisent l'émergence de nouveaux secteurs économiques et transforment en profondeur les activités traditionnelles. Un secteur très récent comme les jeux en ligne né dans les années 1970, par exemple, représentait 35 Md$ en 2013 et atteindra probablement 56 Md$ d'ici à 2018[2].
Mais la numérisation et les interconnexions de toutes natures augmentent également les possibilités d'attaques informatiques. Celles-ci, par leur fréquence et leur sévérité croissantes, constituent une externalité négative venant diminuer les bénéfices de la société numérique. Bien qu'il soit extrêmement difficile à calculer et que les estimations varient, la majorité des études situent en effet le coût global de la cybercriminalité entre 100 Md$ et 500 Md$ par an.
Dans ce contexte de croissance double, celle de l'économie numérique, d'une part, et celle de la cybercriminalité, d'autre part, le marché de l'assurance cyber se développe rapidement, mais reste encore naissant et peu structuré. À quels défis ce secteur est-il confronté ? Quels sont les outils à développer pour assurer sa pérennité et sa profitabilité ?

LES RISQUES CYBER : ENTRE DÉMULTIPLICATION DES MÉTHODES ET STABILITÉ DES CONSÉQUENCES

Les attaques informatiques sont de natures très diverses. La prolifération d'objets connectés semble stimuler l'imagination des attaquants qui réussissent à déjouer la sécurité (quand elle existe...) de la plupart des nouveaux systèmes. Ainsi il est, par exemple, possible de retrouver le mot de passe d'un réseau Wifi grâce aux ampoules électriques connectées qui se l'échangent « en clair » (c'est-à-dire sans sécurité). Plus grave, en octobre 2016, une attaque informatique ayant utilisé des caméras connectées a bloqué l'opérateur informatique Dyn, ce qui a mis hors ligne pendant plusieurs heures de nombreux services et médias en ligne comme Verizon Communications, CNN, Fox News, Twitter, Netflix sur la côte est des États-Unis.
Ces attaques émanent d'acteurs aux capacités très différentes. Il peut s'agir d'employés mécontents cherchant à profiter de leurs accès privilégiés pour se venger de conditions de travail qu'ils jugent inacceptables ou pour voler des informations sensibles (base de clients, brevets). À l'autre bout du spectre, parmi les acteurs les plus sophistiqués et organisés, des États conduisent des opérations dans le cyber-espace visant à collecter du renseignement ou à entraver le fonctionnement des infrastructures critiques d'un pays. Il est probable que la coupure électrique survenue en Ukraine en décembre 2015 fasse partie de cette catégorie. Cette cyber-attaque sophistiquée contre trois centrales de génération électrique a plongé environ 100 000 foyers de l'ouest de l'Ukraine dans le noir pendant plusieurs heures[3]. De même, les attaques informatiques de 2012 qui ont permis de voler le design de systèmes d'armes américains, comme l'avion de chasse F-35 ou le système antimissile AEGIS, sont probablement d'origine étatique. Enfin il est

possible que la cyber-attaque ayant touché une aciérie allemande en 2014 et ayant causé un arrêt de production et la destruction des fours ait elle aussi été conduite par un État.
Entre ces deux extrêmes, la cybercriminalité représente la grande majorité des cas. Plusieurs exemples récents montrent que les criminels sont organisés, utilisent un large éventail de méthodes d'attaque et réussissent à voler des sommes d'argent très importantes. Le cas de l'attaque du réseau interbancaire SWIFT, survenue en février 2016, est emblématique de ce phénomène[4]. Les attaquants sont entrés dans le système grâce à des informations de connexion volées, ont procédé à des virements, dont l'un de 81 M$ depuis le compte de la banque centrale du Bengladesh, et installé un logiciel malveillant qui efface les traces de ces transactions frauduleuses. On pourrait également citer la vague d'extorsions sans précédent qui a touché les établissements de santé et les universités aux États-Unis depuis le début de 2016, en augmentation de 300 % par rapport à 2015.
Mais sous cette apparente diversité – des ampoules connectées aux opérations militaires –, les impacts des cyber-attaques restent finalement assez stables et peuvent être catégorisés en six domaines : vol de données, extorsion, fraude, modification ou détournement de produits (introduction de virus dans une voiture connectée, par exemple), perturbation d'infrastructures critiques et attaques informatiques donnant lieu à des dommages matériels.

ANALYSER ET QUANTIFIER LES IMPACTS

Pour faire face à la multiplication des attaques informatiques, les organisations ont progressivement installé des mesures de protection. De nombreux outils et services de sécurité informatique ont été mis au point en suivant la logique du glaive et du bouclier : à chaque nouveau type d'attaques, les éditeurs de sécurité ont fourni une contre-mesure sous la forme de logiciels (antivirus, *firewalls,* etc.) ou de services (surveillance et détection d'attaques, réponse aux incidents, etc.). Très *bottom-up* et s'appuyant largement sur des mesures techniques, cette approche laisse de côté l'analyse des impacts *business* et financiers.
C'est sans doute l'une des raisons pour lesquelles les dirigeants ont du mal à s'emparer de ce risque. Pourtant, dans le contexte de numérisation grandissante, analyser les scénarios de « catastrophe cyber » et quantifier leurs impacts sont devenus indispensables.
Ces impacts ne sont pas seulement informatiques : l'indisponibilité des systèmes d'information entraîne des pertes d'exploitation, la diffusion de données personnelles de clients impacte négativement la réputation[5], un virus introduit dans un produit déclenche le rappel de ce produit ou des mises à jour de grande ampleur. Pour quantifier les conséquences financières des incidents cyber, de nombreuses fonctions de l'entreprise doivent donc travailler conjointement, à commencer par les *risk managers*, les responsables opérationnels, les responsables financiers, l'IT (*information technology*), etc. Tous contribuent à définir les scénarios majorants et leurs impacts. Cela demande de dépasser les différences culturelles, ce qui n'est pas simple compte tenu de la technicité de ce risque, et de s'accorder sur une méthodologie structurée pour que les résultats soient reproductibles dans le temps et acceptés par tous.

UNE DYNAMIQUE FAVORABLE AUX ATTAQUANTS SOUTENUE PAR UN CONTEXTE ÉCONOMIQUE TENDU

Alors que les entreprises doivent travailler à l'identification et la réduction des risques cyber, peut-on espérer une diminution des attaques ? Malheureusement la dynamique actuelle laisse envisager une croissance continue du nombre de cyber-attaques dans les années à venir pour plusieurs raisons structurelles

Une forte tension économique du marché du logiciel, des produits informatiques et des objets connectés

Il reste que ces attaques sont possibles parce que des failles continuent de proliférer dans les logiciels ou les équipements IT, même si certains éditeurs ont fait de très gros progrès pour corriger leurs *bugs* et diffuser rapidement et efficacement les mises à jour de leurs produits. Mais malgré cette amélioration, ce sont encore des milliers de vulnérabilités qui sont découvertes chaque année dans les logiciels et les systèmes d'exploitation les plus courants[6]. Et c'est sans compter les objets connectés qui sont en général très peu sécurisés.
La pression concurrentielle est l'une des principales raisons qui expliquent ce phénomène. Parmi les éditeurs, les entreprises de services IT et les fabricants d'équipement réseau et d'objets connectés, le *time-to-market* et la maîtrise des coûts de production sont absolument critiques. Or mettre en œuvre de la sécurité introduit des délais et des coûts (tests, audits de sécurité, application des correctifs, validation, etc.). Ainsi de nombreux produits ou services sont mis sur le marché sans que leur sécurité ne soit testée et validée.
Ensuite la sécurité n'est pas, en général, un argument de vente très attractif, notamment pour les produits grand public comme les objets connectés. La théorie du « *Market for Lemons* » (Akerlof, 1970) s'applique donc : comme les clients ne savent pas comparer la sécurité de deux produits concurrents, ils vont finalement acheter le moins cher ou baser leur choix sur d'autres critères. La sécurité est vue comme une fonction non essentielle pour séduire la clientèle et n'est donc pas prioritaire dans le développement du produit. Sa qualité tend donc à diminuer au fil du temps.
Enfin les éditeurs de logiciels et les fabricants d'objets connectés ne subissent pas directement les conséquences des failles de sécurité de leurs produits. N'ayant généralement pas d'engagement contractuel de sécurité avec leurs clients, ils ne sont pas incités à améliorer le niveau de sécurité, si ce n'est pour préserver leur image. Ils créent ainsi une « dette de sécurité » qui va augmenter au fur et à mesure de la diffusion du produit car il deviendra de plus en complexe – et donc cher – de corriger ses failles. S'il s'avère, par exemple, que certains pacemakers très répandus ont effectivement des failles de sécurité[7], il sera très compliqué de leur appliquer des correctifs maintenant qu'ils sont portés par de très nombreux patients.

Les attaquants jouissent d'une relative impunité

L'absence de frontières et les différences entre les réglementations nationales facilitent les actes des cybercriminels. Ils masquent leurs traces en transitant par plusieurs pays. Le temps nécessaire aux forces de police pour établir une coopération internationale et remonter leur piste est donc assez long et les preuves numériques auront disparu. Par ailleurs, le Code pénal français (articles 323-1 et suivants) est particulièrement efficace pour lutter contre la cybercriminalité, mais tous les pays n'ont pas ce même degré de précision, ce qui complexifie encore le déroulement des enquêtes.
De plus, il est techniquement très complexe d'identifier avec certitude les criminels. On ne dispose généralement que de preuves indirectes comme la langue ou le type de claviers utilisé par les auteurs du virus ou le site web malveillant qu'ils ont ouvert pour contrôler leur attaque. Ces éléments sont insuffisants pour identifier les auteurs avec certitude, d'autant que les codes informatiques des logiciels malveillants se recyclent ou s'échangent.

Le rôle dual des États

De très nombreux États ont adopté des réglementations visant à protéger les infrastructures critiques et les données personnelles de leurs citoyens contre les attaques informatiques et incitent ainsi les organisations publiques et privées à améliorer leur sécurité.
Mais en parallèle, de plus en plus de pays, dont la France[8], annoncent publiquement développer des capacités militaires et recourir à des actions offensives dans le cyber-espace. Même si elles ont des objectifs très différents de la cybercriminalité, ces activités exploitent également les faiblesses des réseaux et des logiciels. On peut donc s'interroger sur les priorités des

gouvernements entre le besoin de sécuriser leurs citoyens et leurs entreprises, d'un côté, et celui de laisser en place des failles qui facilitent leurs actions militaires et de renseignement, d'un autre côté.

UNE RÉGLEMENTATION QUI SE DÉVELOPPE FACE AUX ENJEUX

Concernant la protection des données personnelles, un cadre réglementaire existe en France depuis 1978 et la création de la CNIL (Commission nationale de l'informatique et des libertés) qui impose des obligations et définit les sanctions en cas de manquement. Le « paquet Télécom » de 2011 y a ajouté des obligations de notification au régulateur et parfois aux victimes, mais pour les seuls fournisseurs de services de communications électroniques. Les États-Unis ont été plus loin en adoptant à partir de 2003 dans la plupart des États, une obligation de notification pour l'ensemble des entreprises. Des lois fédérales complètent le tableau pour les données financières ou de santé avec de lourdes sanctions pécuniaires à la clé. D'autres réglementations sectorielles existent, comme celle imposée par les réseaux de cartes bancaires (PCI-DSS). La réglementation européenne GDPR[9] qui s'appliquera à tous les pays membres de l'Union européenne en mai 2018 imposera aux entreprises de protéger les données personnelles qu'elles détiennent au risque de subir des sanctions allant jusqu'à 4 %de leurs revenus mondiaux.
Au-delà des données personnelles, le régulateur s'intéresse également aux risques des infrastructures vitales pour le fonctionnement de la société. Ainsi, en France, la loi de programmation militaire 2014-2019 adoptée en décembre 2013 impose aux opérateurs d'importance vitale (OIV) la mise en place de mesures de cybersécurité et des mécanismes de remontée d'incidents à l'Agence nationale de la sécurité des systèmes d'information (ANSSI). À l'échelle européenne, la directive NIS (*Network and Information Security*) qui doit être transposée en droit national avant mai 2018 imposera le renforcement de la cybersécurité des opérateurs de services essentiels. Aux États-Unis, des réglementations sectorielles existent également pour certains opérateurs de *critical national infrastructures*.
On le voit, la plupart des États renforcent leur arsenal réglementaire face à la menace cyber. On assiste à une harmonisation régionale (Union européenne en Europe, fédérale aux États-Unis) des obligations et à une extension (territorialité, acteurs, processus) des couvertures réglementaires pour adresser l'ensemble de la chaîne de risques.

L'ASSURANCE DES CYBER-RISQUES : UN MARCHÉ EN CONSTRUCTION

L'assurabilité du cyber-risque

L'assurabilité d'un risque repose sur plusieurs critères.

Il doit être quantifiable

C'est à ce jour une difficulté majeure pour le cyber-risque. Peu de données sont disponibles, car le risque est relativement récent et parce que les entreprises sont réticentes à communiquer sur les attaques.
Le risque le mieux connu est celui de l'atteinte aux données personnelles aux États-Unis, puisqu'il fait l'objet de notifications obligatoires (*cf. supra*). Pour autant, si les données disponibles permettent d'évaluer la fréquence des attaques et le volume de données compromises par secteur d'activité, elles ne fournissent pas de détails sur les impacts financiers pour les entreprises victimes de ces attaques.
Face à ces lacunes et conscientes du besoin, les institutions lancent des initiatives pour la collecte et l'anonymisation des données. Ainsi l'ANSSI a récemment mis en place le dispositif ACYMA d'assistance aux victimes qui comprend un Observatoire du risque alimenté par le recueil des données. La difficulté de ces démarches provient de leur capacité à transformer des données de

bas niveau sur les incidents en informations utilisables par les assureurs (type de risques et quantification des impacts).
Une autre difficulté pour la modélisation du risque provient de sa mutation dans un environnement technologique en pleine expansion. L'expérience passée n'est pas forcément représentative du futur.

Il doit être aléatoire

Ici l'aléa s'entend du point de vue de l'assuré, tant il est vrai que l'essentiel du risque provient de l'acte malveillant. La probabilité de succès de l'attaque repose sur le degré de maturité de la cible et la nature de l'attaquant, mais avec une dissymétrie de moyens plutôt en faveur de l'agresseur. Par ailleurs, les risques se distribuent souvent par vagues (vol de données, rançonnage, etc.) en fonction de la technologie (vulnérabilité d'un logiciel, par exemple) ou de l'environnement géopolitique.
Enfin certaines entreprises emblématiques génèrent un tropisme avéré des « hacktivistes ».
Tous ces facteurs méritent d'être appréciés et modélisés. D'une façon semblable au risque politique ou au risque de guerre, dont le cyber-risque hérite en partie, il pourra s'avérer que sous certaines conditions, les facteurs de menace ou de vulnérabilité feront perdre au risque son caractère aléatoire.

Il faut enfin souligner le caractère potentiellement systémique du cyber-risque

L'interconnectivité grandissante des systèmes, l'utilisation de logiciels ou de matériels standards, l'externalisation croissante des services informatiques créent les facteurs de propagation des attaques et de catastrophes cyber à l'échelle planétaire, qu'il s'agisse de l'exploitation massive d'une vulnérabilité logicielle ou d'attaques ciblées sur des opérateurs qui, par leur position dominante sur le marché ou leur rôle clé dans les infrastructures techniques ou de métier, possèdent un caractère systémique.

PHYSIONOMIE DU MARCHÉ

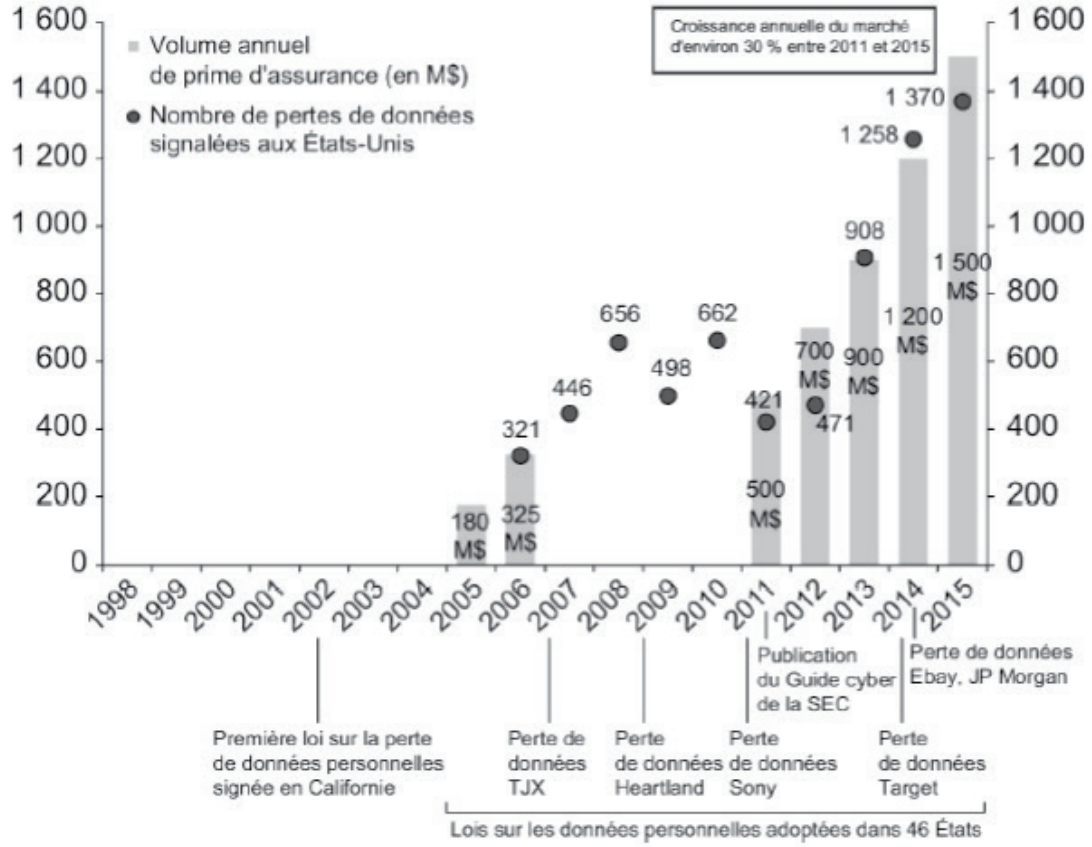
L'assurance des cyber-risques n'est pas si récente. Dès la fin des années 1990, des produits sont apparus aux États-Unis pour couvrir la responsabilité liée aux contenus diffusés en ligne ou aux logiciels à la suite d'une compromission de sécurité informatique. Ces garanties développées à partir des polices de responsabilité civile professionnelle s'adressaient donc aux entreprises du secteur des nouvelles technologies.
Au milieu des années 2000, le développement de la réglementation sur les données personnelles aux États-Unis permet un essor du marché.
Comme il a été évoqué *supra,* à partir de 2003, la plupart des États américains se dotent de réglementations imposant la notification aux victimes de toute compromission de données personnelles. Tout manquement peut être sanctionné par des amendes pouvant atteindre 1,5 M$ ou plus.

Il est intéressant d'observer le cycle vertueux induit par ces réglementations

À l'atteinte aux données personnelles se trouve associé un coût objectif : celui de la notification à des milliers voire des millions d'individus. Cette notification démultiplie aussi le risque de réclamations et d'actions de groupe.
Par ailleurs, la réglementation rend publiques des attaques informatiques, dont certaines majeures, qui étaient auparavant passées sous silence, engendrant une prise de conscience de la part des acteurs économiques.
Prise de conscience et coût du risque favorisent ainsi le développement de nouveaux produits associant la couverture des coûts propres (investigations et réparation des dommages aux

données et aux systèmes informatiques), de la gestion de crise (notification et assistance aux victimes, relations publiques, enquêtes administratives) et des réclamations (frais de défense et indemnisation).
Le marché attire alors de nouveaux clients : banques et institutions financières, grande distribution, éducation, santé. Toute entreprise ayant à traiter en nombre des données personnelles s'intéresse au marché de l'assurance cyber.
Ces dernières années, le marché s'est développé selon plusieurs dimensions.
En premier lieu, des attaques à fort retentissement ont rendu plus aigüe la perception du risque par les entreprises, favorisant l'achat d'assurance.

Graphique 1
Évolution du marché de l'assurance cyber aux États-Unis



Source : AON Inpoint for SCOR.

En deuxième lieu, la dépendance toujours plus forte des sociétés à l'égard des systèmes informatiques et des réseaux et de nouvelles formes d'attaques ciblant les processus industriels ont élargi le marché et les produits. Des garanties de perte d'exploitation à la suite d'une panne informatique d'origine accidentelle ou malveillante sur les systèmes propres à l'entreprise ou ceux de ses prestataires (hébergeurs de données, fournisseurs de services logiciels, infogérance, etc.) sont aujourd'hui proposées par les assureurs et attirent de nouveaux clients (industries de transformation et de production, utilités (eau, énergie), transport).
En troisième et dernier lieu, le marché s'étend dans sa géographie. S'il reste à ce jour majoritairement nord-américain (90 % des primes d'assurance), il se développe en Europe et en Asie. À ce titre, le marché exprime de grandes attentes envers les nouvelles réglementations européennes (GDPR, NIS) mentionnées *supra* et qui pourraient jouer le rôle de catalyseurs observé aux États-Unis.
De fait, le taux de pénétration reste encore relativement faible. Aux États-Unis, s'il est proche de 50 % pour les entreprises de services les plus exposées (services financiers, santé, éducation,

commerce), il reste encore modeste dans l'industrie (10 % à 20 %). En Europe, la pénétration est plus faible. À la fin de 2016, seules la moitié des entreprises du CAC 40 avaient souscrit une police d'assurance cyber. S'agissant des PME (petites et moyennes entreprises), le taux d'achat reste encore très limité à ce jour.

Le marché actuel est de taille modeste. On estime la prime d'assurance mondiale à environ 3 Md$. C'est cependant un marché à fort développement, puisque les divers analystes prévoient des taux annuels de croissance de 20 % à 40 % pour les prochaines années qui pourraient porter le niveau de prime à 10 Md$ en 2020 et à 20 Md$ en 2025.

Le nombre d'assureurs sur ce marché est en constante augmentation. Aux États-Unis, on estime qu'environ soixante compagnies offrent des produits cyber dédiés. Ce marché reste cependant concentré, puisque les trois premiers assureurs américains (AIG, Chubb, XL Group) généraient à eux seuls 45 % des primes américaines en 2015. Le marché du Lloyd's est l'un des plus actifs sur le marché mondial : plus de soixante syndicats ont produit une prime supérieure à 300 M£ en 2015, capturant notamment 30 % du marché américain. En Europe continentale, la plupart des grands assureurs européens et internationaux se partagent un marché ne dépassant guère 100 M€ de prime.

L'offre de réassurance reste pour le moment en retrait. Le marché a généré environ 500 M$ de prime en 2015. L'absence de modèle de tarification fiable et surtout de modélisation des cumuls de risque crée une certaine prudence des acteurs. Pour ces raisons, l'offre de réassurance est essentiellement proportionnelle et les réassureurs introduisent fréquemment des limites par événement ou annuelles. Alors que le marché de l'assurance se développe à bon train, une capacité de réassurance restreinte pourrait bien vite apparaître comme un frein, si la connaissance du risque ne progresse pas dans les années qui viennent.

UNE OFFRE PRODUIT EN PHASE D'ADAPTATION

Comme indiqué *supra*, le marché a subi de constantes adaptations pour appréhender un risque de plus en plus pervasif et multiforme. Les produits d'assurance cyber reflètent ces mutations. Ils combinent des garanties dommages et responsabilité pour les conséquences matérielles et immatérielles des événements cyber.

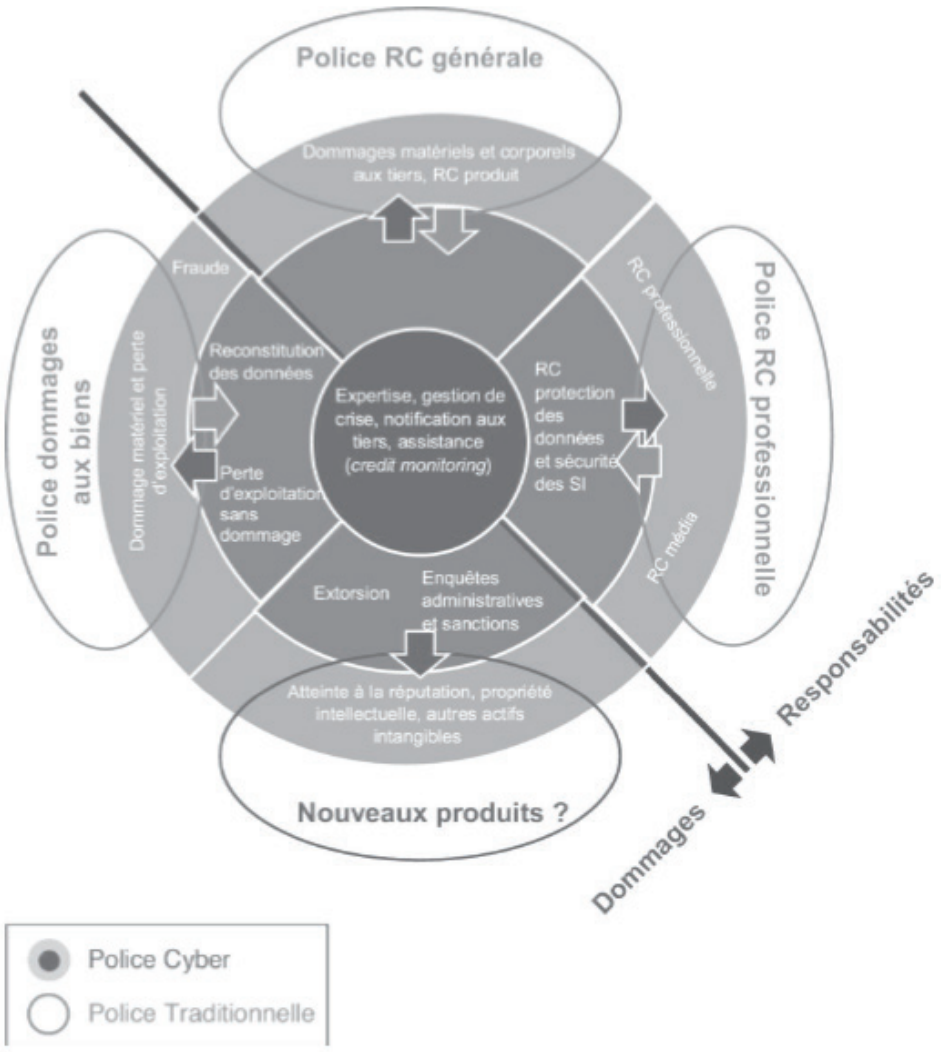
Au-delà des produits spécifiques, les cyber-risques peuvent engendrer des sinistres au titre des polices d'assurance classiques : un incendie ou une explosion seront généralement couverts par une police dommages tous risques. De même, une police de responsabilité civile répondra pour les dommages corporels ou matériels occasionnés aux tiers.

Ces couvertures dites « silencieuses », même si elles se sont peu manifestées à ce jour, créent des interrogations chez les assureurs quant au degré d'exposition de leurs portefeuilles au risque cyber.

Cette perméabilité des diverses polices d'assurance – traditionnelles ou spécifiques – induit des tendances contradictoires sur les politiques de couverture face au risque et, par voie de conséquence, sur le développement des produits.

D'un côté, l'approche *a minima* consiste à élargir les couvertures des polices standards par des rachats d'exclusion ou des extensions de garantie cyber. D'un autre côté, certains assurés optent pour l'achat de polices spécifiques étendues offrant sur base de péril dénommé un grand nombre de garanties normalement couvertes par les polices traditionnelles. Cette alternative a le mérite d'une plus grande clarté quant au degré de couverture de l'entreprise. Elle se heurte néanmoins aux capacités encore limitées offertes par le marché spécialisé cyber.

Graphique 2
Les garanties offertes par les polices cyber et les polices traditionnelles



Source : SCOR.

On le voit, la cyber-assurance est encore en quête de maturité. Comme pour tout marché d'assurance, ce processus de maturation est le fruit d'une symbiose entre connaissance et maîtrise du risque par les assurés, environnement réglementaire adapté et développement de l'expertise et des produits par les assureurs et les réassureurs.

LE PÉRIL CYBER : RÉVÉLATEUR DES NOUVEAUX RISQUES DU XXIe SIÈCLE

Les actifs intangibles sont au cœur de l'entreprise

Les cyber-risques touchent l'entreprise en son sein. Ils visent en premier lieu ses actifs immatériels. Des attaques de grande ampleur ont révélé la fragilité de grands groupes face à l'écho médiatique : perte de confiance des clients, atteinte à la marque. Ce n'est pas l'apanage des cyber-risques, l'affaire Volkswagen est là pour nous le rappeler. Mais cela révèle que les actifs intangibles (capital intellectuel, réputation, brevets, marques, données, etc.), alors qu'ils pèsent parfois pour plus de la moitié de la valeur de l'entreprise, ne trouvent aujourd'hui aucune réponse assurantielle satisfaisante.

Le numérique bouleverse le profil des risques traditionnels

Avec les objets connectés, nous assistons à l'irruption de la robotisation et de l'automatisation dans les produits et les services les plus courants. Le mariage de la nouvelle économie et de l'industrie traditionnelle (automobiles, biens domestiques) fait de la cybersécurité un enjeu auquel les développeurs, les fournisseurs de solutions et les intégrateurs ne pourront se soustraire. En effet, l'irruption du digital dans le monde physique induit de nouveaux périls matériels et corporels et les impératifs de sécurité et de sureté (par exemple, dans les transports ou la santé) modifient la tolérance au risque. La nouvelle économie va devoir s'adapter et son environnement juridique également. Le « droit à l'erreur » et les limitations de responsabilité des entreprises de nouvelles technologies qui visaient à favoriser la R&D (recherche et développement) vont se trouver questionnés par ces changements. Cela crée le germe d'une révolution à venir dans la chaîne de responsabilités et dans l'exposition au risque de ces entreprises.
Par ailleurs, cette même digitalisation de la vie courante va induire un déplacement des risques de la défaillance humaine vers la malveillance.
Ces transformations vont bouleverser les portefeuilles traditionnels des acteurs de l'assurance et de la réassurance. Sur le marché des particuliers, par exemple, (automobile ou accidents de la vie), on devrait constater une réduction drastique des risques dus aux facteurs humains et une augmentation des menaces et des risques systémiques.

La technologie modifie le paysage des risques majeurs

Aujourd'hui, l'assurance et la réassurance identifient les catastrophes naturelles et les pandémies comme étant les principaux risques majeurs auxquels elles doivent faire face, mais les risques technologiques pourraient bien changer la donne dans les années qui viennent.
En effet, le numérique connecte à la toile tous les domaines de la vie et des activités humaines, créant une vaste surface d'exposition. Dans le même temps, les moyens et les capacités de nuire dans ce cyber-espace vont croissants.
La grande porosité entre acteurs malveillants (États, terroristes, criminels, hacktivistes) et les modalités d'attaque rendent l'attribution et la qualification des actes de plus en plus difficiles, voire impossibles.
Cela questionne la segmentation traditionnelle des marchés d'assurance non-vie qui distingue classiquement accidents d'origine humaine ou naturelle, risques de guerre, terrorisme, risques politiques.
Dans le même temps, et alors qu'aucune menace technologique n'a encore impacté à grande échelle nos sociétés, les acteurs sont face à l'impérieuse nécessité d'appréhender et de quantifier les événements majeurs pour évaluer leur degré de résilience : « penser l'impensable ».
Ce processus pourrait conduire à la mise en place de groupements ou d'autres structures avec garantie de l'État, afin de répondre aux évènements technologiques d'intensité exceptionnelle, quelle qu'en soit l'origine, qui ne pourraient être portés par le seul marché commercial.
Au-delà des cyber-risques, c'est toute l'économie du risque qui doit être repensée, afin de prendre en compte les changements à venir induits par la technologie dans la vie des entreprises et des particuliers.

NOTES

1. Voir le site : http://ir.aon.com/about-aon/investor-relations/investor-news/news-release-details/2017/AonPonemon-report-Almost-four-times-more-budget-is-being-spent-on-property-related-risks-vs-cyber-risk/default.aspx.
2. Voir le site : http://www.statista.com/statistics/270728/market-volume-of-online-gaming-worldwide
3. Voir le site : http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.
4. Voir le site : https://www.swift.com/insights/press-releases/swift-customer-communication_ customer-security-issues.
5. Alors que Verizon était en train de racheter Yahoo, la révélation de la perte de plus de 1 milliard d'informations personnelles de clients de Yahoo a conduit à une baisse de la transaction d'un montant de 350 M$. Voir le site : http://money.cnn.com/2017/02/21/technology/yahoo-verizon-deal/
6. Voir le site : https://www.cvedetails.com/top-50-products.php?year=2016
7. Voir, par exemple, le site : http://d.muddywatersresearch.com/wp-content/uploads/2016/08/MW_STJ_08252016_2.pdf ou le site : http://www.reuters.com/article/us-cybersecurity-medicaldevices-insight-idUSKCN0IB0DQ20141022.
8. Voir le Livre blanc sur la défense et la sécurité nationale 2013, p. 107.
9. General Data Protection Regulation, voir le site : http://www.consilium.europa.eu/fr/policies/data-protection-reform/data-protection-regulation/.

BIOGRAPHIES

Didier Parsoire est directeur du département Cyber Solutions de SCOR Global P&C.

Commençant sa carrière comme ingénieur Spatial, Didier a rejoint SCOR en 1992 en tant que souscripteur Risques Spatiaux et a pris la responsabilité du département Spatial quelques années plus tard. Il a occupé plusieurs fonctions managériales dans la souscription des grands risques depuis les entreprises de nouvelles technologies jusqu'aux captives et solutions structurées. Plus récemment, il a initié la conception d'un système avancé pour la souscription des grands risques avant de prendre en charge les opérations Cyber en 2014. Didier est ingénieur diplômé de Supaero.

Sébastien Héon est directeur adjoint du département Cyber Solutions de SCOR Global P&C.

Sébastien a commencé sa carrière comme professeur de mathématiques puis a rejoint le ministère de la Défense en tant qu'expert en cryptologie. Il devient conseiller pour les relations internationales à l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) puis rejoint Airbus en 2009 comme responsable de la division Cybersecurity Advisory. Jusqu'en 2013, il est également professeur associé de cryptologie à l'université Paris Diderot.