UNIVERSITE JEAN MOULIN LYON III

Institut des Assurances de Lyon

Master 2 Droit des assurances

Roxanne DESLANDES

Présentation des programmes de cyberassurance et de leurs limites

2016-2017

Sous la direction de Monsieur Philippe VEZIO

UNIVERSITE JEAN MOULIN LYON III

Institut des Assurances de Lyon

Master 2 Droit des assurances

Roxanne DESLANDES

Présentation des programmes de cyberassurance et de leurs limites

2016-2017

Sous la direction de Monsieur Philippe VEZIO

Synthèse

Les programmes de cyberassurance forment une réponse adaptée au risque cyber parce qu'ils couvrent les dommages subis par l'assuré et les dommages subis par les tiers, tout en fournissant à l'assuré des prestations d'assistance et de gestion de crise. Les assurances traditionnelles n'apportent pas une telle réponse à ce risque parce qu'aucune d'entre elles n'est d'une nature mixte.

Le cyber assureur doit persister dans l'innovation de son métier en transformant la gestion de crise en gestion de risque et en repensant la souscription de ce risque complexe, notamment par secteur d'activité. L'assureur, par son point de vue panoramique sur les sinistres cyber et son rôle central dans la gestion de risque, peut contribuer à la cyber résilience en incitant l'assuré à améliorer sa gouvernance de risque et en dynamisant les relations avec les divers acteurs du processus.

Les programmes de cyberassurance, dans leur généralité, ne couvrent pas l'ensemble des conséquences d'une cyber atteinte puisque les dommages matériels n'en sont pas couverts. Cela conduit à des éventuels cumuls d'assurance avec les programmes traditionnels ou des absences de garantie.

L'absence d'exclusion du risque cyber dans de nombreuses polices traditionnelles amène à une dangereuse problématique d'accumulation de risque qui n'est, par son aspect silencieux, pas maîtrisée par les mécanismes de financement de l'assurance, et sous-tend une problématique de solvabilité des assureurs et plus encore des réassureurs. Les mécanismes de modélisation et d'agrégation du risque doivent à l'avenir permettre un meilleur management de l'accumulation de ce risque.

Remerciements

Je remercie l'Institut des Assurances de Lyon grâce auquel j'ai pu saisir l'opportunité de réaliser mon mémoire de fin d'études sur la cyberassurance.

Je remercie Philippe VEZIO, Financial Lines Managing Director chez Tokio Marine HCC, pour m'avoir accompagnée durant toute mon étude et s'être tenu accessible et intéressé.

Je remercie Xavier MARGUINAUD, Cyber Underwriting Manager chez Tokio Marine HCC, pour son expertise, sa disponibilité et ses nombreux conseils.

Je remercie Nacira GUERROUDJI-SALVAN, Présidente du Cercle des Femmes dans la cybersécurité (CEFCYS), pour son dévouement à la cybersécurité et sa volonté de faire progresser les juniors.

Sommaire

Introduction

La violation de données à caractère personnel la plus importante aujourd'hui connue a été dévoilée le 3 avril 2016. Il s'agissait de la soustraction auprès de l'entreprise panaméenne Mossack Fonseca de plus de deux térabytes de données fiscales confidentielles relatives à l'existence de comptes offshore au Panama. 11,5 millions de documents confidentiels couvrant une période des années 1970 à l'année 2015 ont été rendus publics par un certain « John Doe », un initié anonyme. Cela concernait 4,8 millions d'emails, 3 millions de bases de données, 2,2 millions de fichiers PDF, 1,1 million d'images et 320 000 documents textes. Le but de cette opération était de mettre en lumière les inégalités de revenus en dévoilant comment des personnes connues dans plus de quarante pays incluant le Royaume-Uni, la France, la Russie, la Chine et l'Inde, cachaient leurs ressources et évitaient de payer des taxes dans leurs propres pays en créant des comptes et des entreprises coquilles vides au Panama. Les répercussions politiques de ce scandale ont été conséquentes puisque le Premier ministre islandais et le Ministre de l'industrie espagnol ont démissionné, notamment. Soixante-douze chefs d'Etat ont été nommés dans cette fuite de données, ainsi que des centaines de personnes de haut-rang officiel au sein de gouvernements nationaux, tout comme des personnes notoirement aisées, leurs proches et leurs associés.[1]

L'exposition de chacun au risque cyber, personne physique ou personne morale, est une évidence aujourd'hui. La digitalisation, la robotisation, le *Bring Your Own Device*, l'avènement des objets connectés, de la domotique, du *cloud computing*, amènent chacun des acteurs économiques à devenir cyberdépendants dans le quotidien de leur vie publique et de leur vie privée, et sont autant de portes ouvertes aux cyberattaques. Les nouveaux moyens de communication, technologies et systèmes d'information sont une telle source de développement économique qu'il est souvent fait référence à la quatrième révolution industrielle,[2] mais rendent les valeurs immatérielles, et vulnérables.

81% des entreprises françaises ont été visées par une cyberattaque en 2015 et le nombre des cyberattaques a augmenté de 51% en une année.[3] Les entreprises, qui ont

[1] CENTRE FOR RISK STUDIES, University of Cambridge Judge Business School & Risk Management Solutions (RMS), *2017 Cyber Risk Landscape*, 12 p.
[2] WORLD ECONOMIC FORUM, *The Global Risks Report 2016*, 11th edition, 2016, 9 p.
[3] AIG, Conférence sur la cyberassurance, Paris, Mars 2017.

digitalisé la relation-client-fournisseur et les relations internes, sont principalement menacées par des groupes financés et professionnalisés qui agissent à l'international. Le *cyber hacking*, consistant en l'introduction malicieuse dans un système informatique,[4] possède une dimension politique. Les revendications sociales sont facilitées par les outils numériques qui maximisent la portée du message citoyen et la rapidité des mobilisations de masse. Le cyber activisme transcende le champ politique traditionnel.[5] La majeure partie de cette activité considérée comme illégale dans de nombreux Etats est organisée et hébergée au sein de pays appelés « paradis numériques », c'est-à-dire dont la législation numérique est inexistante et/ou lesquels n'ont conclu aucun accord numérique à l'international. Lorsqu'il est prohibé, le cyber crime ou le cyber délit reste aujourd'hui encore très peu réprimé.[6] Le rapport gain/risques est plus élevé que pour les infractions matérielles, car il est plus facile pour l'auteur de cacher son identité et d'échapper aux poursuites. La « cybercriminalité », au regard de la « criminalité » matérielle, bénéficie d'une réprobation plus faible de la société civile lorsque cette dernière peine à cerner l'ampleur de conséquences d'une cyber atteinte,[7] voire même, lorsqu'elle la plébiscite ou du moins l'avalise.[8] Pourtant, les dernières cyberattaques ont considérablement excédé les plus larges attaques précédemment observées en termes de magnitude,[9] et sont même rendues vénales par le *darknet*.[10]

Par un acte de malveillance, par négligence ou simplement par erreur, il est possible d'atteindre le système d'information et/ou les données qu'il contient. En effet, une moitié des

[4] L'intrusion est effectuée à l'insu de celui qui exploite le système d'information et traite les données qui y sont contenues. Cette intrusion peut cause des dommages au système d'informations et/ou aux données qu'il contient.
[5] WORLD ECONOMIC FORUM, *The Global Risks Report 2016*, 11th edition, 2016, 46 p.
[6] CENTRE FOR RISK STUDIES, University of Cambridge Judge Business School & Risk Management Solutions (RMS), *2017 Cyber Risk Landscape*, 7 p.
[7] Voir les campagnes de responsabilisation du grand public quant au piratage de films sur DVD et l'application de la notion de vol aux données alors que cette infraction demeure matérielle, étant définie par le Code pénal français comme la soustraction frauduleuse de la chose d'autrui.
La société civile ignore la possibilité que des cyber atteintes puissent produire des dommages immatériels et matériels.
[8] Nous pouvons citer à titre d'exemple le scandale des Panama Papers encore ou même la récente *hacking saga* du groupe HBO dans la diffusion de la saison 7 de la série Game of Thrones. Le groupe de hackers OurMine a pris le contrôle des comptes Twitter et Facebook du groupe HBO en publiant un message précisant qu'ils « testaient » la sécurité et qu'ils proposaient leurs services pour l'améliorer. Précédemment, 1,5 térabyte de données a été soustrait à HBO, incluant un épisode non diffusé et rendu accessible sur Internet avant sa date de diffusion officielle, après demande de rançon. HBO Espagne a de même diffusé par erreur l'épisode 6 de la saison, alors accessible sur Internet avant sa diffusion aux Etats-Unis.
[9] CENTRE FOR RISK STUDIES, University of Cambridge Judge Business School & Risk Management Solutions (RMS), *2017 Cyber Risk Landscape*, 10 p.
[10] Des définitions sont présentées au *Lexique*.

sinistres cyber est causée par la malveillance, l'autre moitié par le facteur humain.[11] Le facteur humain peut notamment consister en la mauvaise sécurisation et gestion du système d'information, mais aussi en l'absence de conscience du risque cyber et des pratiques fondamentales de cybersécurité. Les conséquences, matérielles et immatérielles, en sont tout autant désastreuses : violation de données de valeur - d'entreprise, de propriété intellectuelle, à caractère personnel, bancaires -, perte d'image, pertes d'exploitation, cyber extorsion, explosion…[12] Neuf semaines sont nécessaires pour réparer les conséquences d'un sinistre cyber et le coût total moyen d'une atteinte à la sécurité des données s'élève à 4 millions de dollars américains.[13]

Le transfert non autorisé de données en provenance d'un système d'information, de manière manuelle par une personne avec un accès physique au système ou de manière automatisée par un programme informatique malicieux, continue d'être la cause cyber prédominante de dommages immatériels.[14]

La cybersécurité, ou, *stricto sensu*, comment sécuriser les systèmes d'information, est ainsi un sujet vital pour tout acteur qui traite informatiquement des données. Il s'agit d'un véritable sujet de direction et de gouvernance, faisant partie d'un processus plus global de résilience. Elle est devenue un enjeu économique, stratégique et politique pour les Etats. Selon les estimations, la cybercriminalité coûte à l'économie mondiale 445 milliards de dollars américains, ce qui est plus élevé que de nombreux revenus nationaux. Le risque cyber est un risque global.[15] Si l'événement incertain se réalise, les dommages causés peuvent être significatifs et impacter l'économie de plusieurs pays et industries sur plusieurs années. Les risques globaux ne connaissent pas de frontières géographiques.[16] La cyber résilience est à la source d'un renforcement réglementaire et législatif tant au niveau national qu'international.

L'appréhension du risque cyber et la protection des données et des systèmes d'information passe indéniablement par la technique. Cette protection technique est toutefois

[11] MOUNIER, Lucien, souscripteur cyber chez Beazley, Formation cyberassurance, Paris, Juin 2017.
[12] Nous constaterons plus en avant qu'il est possible qu'une atteinte cyber produise des dommages matériels, compris comme matériels et corporels, lorsqu'elle concerne un système d'information opérationnel notamment.
[13] AIG, Expertise Sinistres, *Assurance cyber : analyse des principales tendances, Livre blanc sur la criminalité*, 4 p.
[14] CENTRE FOR RISK STUDIES, University of Cambridge Judge Business School & Risk Management Solutions (RMS), *2017 Cyber Risk Landscape*, 10 p.
[15] WORLD ECONOMIC FORUM, *The Global Risks Report 2016*, 11th edition, 2016, 11 p.
[16] En annexe : WORLD ECONOMIC FORUM, *The Global Risks Report 2016*, 11th edition, Schéma, 2016, 3 p.

perméable et se complexifie à mesure que l'interconnectivité des systèmes et la cyberdépendance augmentent.[17] Face au sinistre que constitue une cyberattaque ou un cyber incident, potentiellement systémique, l'assurance est un mécanisme de pérennité complémentaire à la cybersécurité, et s'ancre pleinement dans le processus de cyber résilience. La cyber résilience est une approche globale du cyber risque qui implique le facteur humain et les technologies de l'information dans une vision préventive et corrective à court, moyen et long terme. L'assurance est un mécanisme pécuniaire et contractuel qui permet la fourniture de prestations de services à la réalisation du risque en contrepartie du paiement d'une prime ou d'une cotisation. La réponse assurantielle est toutefois traditionnellement cantonnée à la prestation de transfert financier. Pourtant, modéliser le risque cyber alors que sa nature même est extrêmement évolutive et l'appréhender tant dans sa prévention que dans sa gestion *post-event*, c'est participer de sa compréhension et de sa bonne gouvernance. L'assurance doit permettre de transférer le risque cyber résiduel, mais aussi, de le réduire. Elle est au cœur de la maîtrise de risque.

Face à la digitalisation de l'économie et à l'essor des cyberattaques, le marché de l'assurance, d'abord anglo-saxon puis mondial, a développé des offres spécialisées de cyberassurance, en parallèle des extensions de couverture cyber apparues dans les lignes d'assurance traditionnelles mais n'apportant toutefois pas une réponse globale au cyber risque. AIG, ACE, XL, CNA, Beazley ont été les premiers à se positionner sur le marché français. En 2013, Allianz et AXA ont proposé des contrats spécifiques de cyberassurance. En 2011, le portail interactif Play Station Network de Sony a été piraté et les données à caractère personnel de 100 millions d'utilisateurs ont fuité. La juridiction de l'Etat de New-York a rejeté la réclamation en indemnisation de Sony Corporation à l'encontre de ses compagnies d'assurance Zurich American et Mitsui Sumitomo, estimant que la police de responsabilité civile visée ne couvrait pas les préjudices résultant de l'exfiltration et de la divulgation de données à caractère personnel par des pirates informatiques. Sony Corporation a ainsi été tenue débitrice de centaines de millions de dollars de pénalités et coûts associés[18] pendant que le marché de la cyberassurance prenait son envol à l'international.

[17] Selon une étude portée par Trustware en 2016, 97% des applications ont une ou plusieurs vulnérabilités de sécurité.
[18] BAUME, Thomas, *Piratage informatique : le tribunal de New York donne raison aux assureurs de Sony, L'Argus de l'assurance*, Juillet 2014.

Les contrats spécifiques de cyberassurance ont pour ambition de protéger les assurés contre les atteintes au système d'information et/ou aux données qu'il contient et d'apporter une réponse adaptée à un risque complexe. Le terme d'« atteinte », repris dans la plupart des conditions générales des cyberassurances, est neutre quant au fait générateur, qui peut être une cyberattaque ou un cyber incident, impliquant ou non une intention de nuire, sous la réserve des exclusions de risque qui sont plus ou moins propres à chaque assureur. Une exclusion de risque d'une police de cyberassurance peut par exemple porter sur les atteintes au système d'information et/ou aux données causées par une panne informatique. Le terme d'atteinte est assez large pour englober tout type de mutation du système d'information ou de la donnée. La sécurité d'un système d'information et des données contenues est évaluée selon trois critères : la disponibilité, l'intégrité et la confidentialité. Lorsque l'un de ces éléments est remis en cause, le système d'information et/ou les données qu'il contient sont atteints. Les données sont atteintes lorsqu'elles sont sans autorisation altérées, supprimées ou divulguées. Le système d'information est atteint lorsque sans autorisation il est introduit, qu'il est indisponible ou qu'il dysfonctionne.[19]

Le mécanisme contractuel permet aux assureurs de définir librement les risques et garanties ainsi que le fonctionnement du contrat dans la limite du respect de la loi. La prise en charge du risque cyber diffère donc indéniablement d'un assureur à l'autre par la définition des garanties accordées, les plafonds, les franchises, les sous-limites, les exclusions.

Nous allons présenter la structure globale de ces programmes de cyberassurance et les distinguer des polices traditionnelles, afin de cerner l'intérêt de souscrire un contrat spécifique de cyberassurance.

Les clients « grands comptes », particuliers ou entreprises, sont aujourd'hui couverts. Les petites et moyennes entreprises ainsi que la grande majorité des particuliers ne sont pas ou peu couverts par un contrat de cyberassurance alors qu'ils sont tout autant visés par des cyberattaques et sujets à des cyber incidents. Ces derniers sont souvent novices en matière de cybersécurité et de fait, en cyber résilience aussi.

La souscription d'un contrat de cyberassurance ne comble cependant pas l'ensemble des atteintes des assurés quant à prise en charge par l'assurance du cyber risque, et s'expose à

[19] ALAU, Ingrid, *Mémoire de recherche, Les cyber-risques dans l'entreprise : enjeux et assurance*, Master 2 Droit des assurances, Institut des Assurances de Lyon, 2013.

plusieurs limites. Le marché de la cyberassurance doit relever deux principaux challenges : innover la souscription et la gestion de risque cyber, gérer la problématique du cumul sur les portefeuilles cyber et sur les portefeuilles globaux tout en positionnant la capacité afin de faire face au fort potentiel catastrophique du risque cyber.

L'assureur doit repenser son métier afin de maîtriser le risque cyber. Nous allons, tout en cernant les limites des programmes de cyberassurance, porter la réflexion sur d'éventuels axes d'amélioration et perspectives d'évolution de la cyberassurance. Nous constaterons alors que le cyber assureur peut se positionner comme la pierre angulaire du processus de cyber résilience tant nécessaire à l'appréhension du cyber risque, complexe et protéiforme.

I La présentation du contrat de cyberassurance

L'assurance est un des piliers de pérennité mais aussi de protection des entreprises. Constituant traditionnellement une prestation de transfert financier du souscripteur à l'assureur, elle se fait face au cyber risque une offre de garanties adaptées et de services de gestion de crise. L'appréhension du risque cyber par l'assurance demande de fournir des garanties dommages[20] et des garanties de responsabilité. Nous étudierons tout l'enjeu de l'adaptation de ces garanties au cyber risque. Cette nature mixte particulière au contrat de cyberassurance distingue ce dernier des autres contrats d'assurance qui pourraient éventuellement s'appliquer au risque cyber, sans toutefois en apporter une réponse globale. Nous constaterons cependant que les lignes traditionnelles restent dans la perspective du risque cyber, et peuvent venir, hélas en cumul, mais aussi en complément de couverture d'une police de cyberassurance. En effet, nous constaterons qu'une cyberattaque ou un cyber incident peut causer des dommages matériels et que ces derniers sont généralement exclus de la couverture des polices cyber, sans pour autant ne pas être pris en charge par les polices traditionnelles, du fait de leur exposition affirmée ou silencieuse au cyber risque.

A Un contrat d'assurance mixte novateur

Le contrat d'assurance cyber est une couverture en « Périls Dénommés », c'est-à-dire qu'il prend en charge uniquement les risques qui y sont explicitement définis, en excluant de fait tout le reste.

Le risque cyber est complexe et protéiforme, le contrat d'assurance doit donc disposer de plusieurs volets pour appréhender ses diverses typologies et ses diverses conséquences. L'idée est d'assurer les dommages subis par les tiers et les dommages subis par les assurés.

[20] Le terme d'assurance dommages n'est juridiquement pas exact puisque les assurances de dommages, qu'elles soient indépendantes ou comprises dans un contrat mixte, sont opposées aux assurances de personnes, les unes protégeant le patrimoine de l'assuré, les autres sa personne. Par principe, les assurances de dommages sont indemnitaires alors que les assurances de personnes sont forfaitaires. Les assurances de dommages recouvrent les assurances de responsabilité, qui prennent en charge les dettes de l'assuré, et les assurances de choses qui en protègent l'actif. Les assurances et garanties de dommages évoquées dans ce mémoire sont des assurances de choses, mais les assureurs usent de ce terme pour distinguer les assurances de choses des assurances de responsabilité civile.

Ces volets sont des volets d'assurance, mais aussi de prestations de services d'assistance, d'expertise et de conseil.

Le contrat de cyberassurance est un contrat « *pick and choose* », c'est-à-dire à tiroirs. Les différentes garanties au sein des volets dommages et responsabilité civile sont proposées à la souscription, afin de s'adapter au profil technique et contractuel du client. Le même besoin d'adaptation s'exprime quant aux prestations de services de gestion de crise.

1 Les garanties standards

Il s'agit des garanties qui se retrouvent dans la plupart des contrats de cyberassurance et qui forment la structure « *first and third party* » du contrat de cyberassurance.

a) Les garanties dommages

Les garanties dommages viennent couvrir les pertes de l'assuré suite au sinistre, en dehors de toute réclamation de tiers.

L'assureur cyber prend à sa charge, dans la globalité des offres de cyberassurance, les frais de restauration de données et de remise en état du système d'information, les frais de notification, les frais de surveillance, les frais d'enquêtes et de sanctions administratives, les frais de cyber extorsion, et les pertes de revenus consécutives au sinistre.

Suite à un sinistre cyber, il est en effet nécessaire pour l'assuré et l'assureur de déterminer la cause de l'événement et l'étendue des dommages, afin d'endiguer le sinistre, dans l'idéal d'en minimiser les conséquences, et d'entrer dans le processus de réparation, et voire même, nous le verrons, d'amélioration.

Les garanties de dommages sont activées par le fait dommageable. Il faut agir rapidement si nous voulons limiter les conséquences d'un sinistre cyber. Les garanties dommages sont donc globalement des garanties d'urgence et sont souvent associées à des prestations de conseil juridique, de relations publiques et d'expertise en cybersécurité. En dehors des pertes d'exploitation, de la cyber extorsion qui est souvent optionnelle bien que standard, et des garanties d'enquêtes et de sanctions administratives, les garanties dommages font partie du volet « assistance et gestion de crise ».

i. Les garanties d'urgence

A la suite d'un sinistre cyber, il est nécessaire de rechercher et de détecter les causes du sinistre. Cette action peut être réalisée par du personnel compétent en interne ou par un prestataire d'expertise informatique. L'assureur cyber peut prendre en charge ces frais. Au titre des prestations de gestion de crise, l'assureur peut être en position de mettre en relation l'assuré avec un service d'expertise informatique, et voir, de coordonner les opérations.

Sont ensuite impliqués des frais de reconstitution ou de restauration de données ainsi que de remise en état opérationnel du système. Il est nécessaire pour l'assuré de réaliser au préalable des sauvegardes des données de manière régulière et d'établir un déroulement des procédures de sauvegarde afin que ces dernières ne subissent pas de dysfonctionnements le moment où elles sont indispensables. Un assuré manquant de diligence peut être sanctionné par l'assureur en moyen de clauses d'exclusion ou de conditions de garantie.

Lorsque des données bancaires sont atteintes lors du sinistre, l'assureur peut proposer de prendre en charge des frais de *monitoring* c'est-à-dire de surveillance sur le marché de la revente de données et de l'utilisation de ces données dans des transactions bancaires. Au sein du volet gestion de crise, l'assureur peut mettre à disposition de l'assuré et des personnes concernées un service d'assistance sur une période pouvant durer plusieurs années.

L'assuré qui subit un cyber sinistre doit adopter une communication adéquate dès la découverte du sinistre afin de préserver son image auprès de ses prestataires, ses clients et du grand public, et ce indépendamment de l'origine, malveillante ou accidentelle, de l'atteinte. Il est en effet difficile de cerner les conséquences financières d'une perte d'image due à un sinistre cyber au-delà du cercle des personnes atteintes par une violation de données à caractère personnel. C'est pourquoi il faut y remédier au plus tôt en faisant appel à des prestataires de services de relations publiques et de communication qui minimiseront les craintes des entreprises sur cet impact et géreront la crise. L'entreprise touchée par un sinistre cyber manque souvent de recul et risque d'aggraver la situation en ne profitant pas de conseils avisés dans un domaine dans lequel elle n'est peut-être pas experte. Cette observation est aussi valable pour les particuliers, qui sont en général tout autant novices sur ce point. L'assureur prend en charge ces frais de communication, mais nous constaterons qu'il ne positionne pas uniquement comme un assureur traditionnel assumant un transfert financier au

titre d'une assurance de dommages. Il est gestionnaire de crise lorsqu'il met par exemple en relation l'assuré avec des prestataires qualifiés de services de communication.

Cette nécessité de communiquer est exacerbée par l'obligation de notification qui s'applique en cas de violation de données à caractère personnel. Cette obligation de notification des atteintes à des données à caractère personnel est renforcée par le Règlement général européen sur la protection des données à caractère personnel[21] entrant en vigueur le 25 mai 2018. Actuellement, la violation de données personnelles par une entreprise lambda n'est pas sanctionnée par une obligation de notification, au contraire du cas des hébergeurs et des prestataires informatiques. La nouvelle réglementation instaure une obligation élargie de notifier l'atteinte puisqu'elle s'applique à toutes les entreprises, peu important leurs secteurs d'activité.

L'obligation de notifier l'atteinte dans les 72 heures du sinistre jouera dans plusieurs hypothèses. En cas de violation de données personnelles, toute entreprise traitant des données, et non plus seulement les fournisseurs de services de communications électroniques au public, doit notifier à l'autorité compétente, la Commission nationale de l'informatique et des libertés (CNIL) en France, et aux intéressés. En cas d'atteinte aux systèmes d'information des opérateurs de services essentiels et des fournisseurs de services numériques, ces derniers doivent notifier à l'autorité compétente. Cette obligation s'applique pour l'instant aux opérateurs d'importance vitale en faveur du premier ministre et de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).[22]

Les frais de notification sont pris en charge par l'assureur au titre du volet dommages. Le manquement à l'obligation de notifier engage néanmoins la responsabilité du responsable de traitement et peut être couverte par le volet de responsabilité civile du contrat de cyberassurance. L'enjeu de clarifier cette dichotomie est principalement, en France, l'étendue de la garantie dans le temps, car les garanties de responsabilité civile en base réclamation applicables aux risques professionnels sont assujetties au régime légal de l'article 124-5 alinéa 4 du Code des assurances.

Cette obligation de notifier amène à la naissance de risques en cascade : enquêtes administratives, réclamations, recours en justice. Ces risques rendent impérative la fourniture

[21] PARLEMENT EUROPEEN ET CONSEIL, Règlement (UE) 2016/679, 27 avril 2016.
[22] AIG, Autopsie d'un sinistre, Risques de cybercriminalité, classe virtuelle, 30 juin 2017.

de prestations de communication et juridiques, qui aideront l'assureur et l'assuré à minimiser les conséquences du sinistre.

ii. L'option de la cyber extorsion

La cyber extorsion est une garantie dommages d'urgence. Elle aussi demande d'être accompagnée par des prestations de gestion de crise, si non même en est la parfaite combinaison, ce qui justifie son étude particulière. La cyber extorsion est une garantie standard des contrats de cyberassurance mais souvent optionnelle.

La menace d'extorsion est définie par AIG dans son Pack Cyber comme toute demande de remise de fonds faite à l'assuré aux fins d'empêcher ou de mettre fin à une menace à la sécurité du système informatique pouvant aboutir à une atteinte à la sécurité des données et causant un préjudice financier au souscripteur.[23] AIG prend en charge le versement de fonds pour empêcher ou mettre fin à la menace d'extorsion et les frais engagés auprès de tout consultant indépendant pour effectuer une enquête déterminant la cause de la menace. Dans les conditions générales Beazley Breach Response de Beazley, nous pouvons noter que l'assureur prend à sa charge, sous son consentement préalable écrit, les frais que le souscripteur est contraint d'exposer pour mettre fin à la menace d'extorsion, toute perte, destruction, disparition des espèces et biens en cours de transfert pour le compte du souscripteur, et les frais et honoraires auprès de consultants.[24] Cette garantie est confidentielle. En général, sont exclues de la garantie les cyber extorsions impliquant des personnes internes à la cible.

Les hypothèses de cyber extorsion sont relativement rares biens que le nombre de ces événements aient récemment augmenté en fréquence. La cyber extorsion se réalise fréquemment au moyen d'un ordinateur personnel afin d'atteindre des entreprises du *small* et du *middle market*. La demande de rançon est souvent contenue dans un e-mail. Le nombre d'entreprises atteintes est large et le montant de la rançon conséquent. La cyber extorsion prend place dans des cyberattaques par *ransomware*, par lesquelles des *malwares* sont infiltrés dans les systèmes d'information de l'entreprise pour mettre hors d'usage les serveurs et bloquer les données jusqu'à ce que la rançon soit payée. L'année 2016 a été le théâtre de

[23] AIG, Conditions générales Pack Cyber 072014, 25 p.
[24] BEAZLEY, Conditions générales Beazley Breach Response, 17 p.

nombreuses cyberattaques par *ransomware*. L'ampleur de la cyberattaque au moyen du *ransowmare* Wannacry a été telle qu'elle a permis à tout public de prendre conscience des risques cyber et de l'opportunité de souscrire une cyberassurance.

Nous bénéficions de peu de données sur le point de savoir si les demandes de rançon aboutissent effectivement auprès des entreprises, car peu d'entre elles sont prêtes à divulguer cette information. Des alternatives au paiement de la rançon existent toutefois, dans certains cas. Par exemple, en novembre 2016 une attaque avec cyber extorsion a gelé le système de paiement du train de San Francisco en l'attente du paiement d'une rançon de 73 000 dollars. Au lieu de payer cette somme d'argent, la municipalité a préféré laisser les clients utiliser le train gratuitement pendant la reconstitution du système d'information.[25] D'un point de vue pragmatique, il peut apparaître à certains plus rentable, du moins à court terme, de payer le prix d'une rançon que d'investir dans des prestations de décrytage/cryptage et de supporter les frais d'interruption d'exploitation. Cette remarque est éminemment vraie concernant les particuliers. Toutefois, compte tenu de l'augmentation du nombre de cyberattaques et de la vulnérabilité toujours plus grande des données, il est certainement à conseiller d'investir en tout état de cause dans des mesures toujours plus avancées de cybersécurité.

La typologie de cette menace cyber peut justifier la présence de cette garantie au sein du volet gestion de crise. Elle participe de la novation du rôle de l'assureur traditionnel qui ne doit cesser d'être développée.

iii. Les pertes et frais supplémentaires d'exploitation

Une atteinte au système d'information d'une entreprise et/ou aux données contenues cause une baisse du chiffre d'affaires, c'est-à-dire des pertes d'exploitation.

Il s'agit ici de considérer les conséquences financières de la perte d'image de l'entreprise sinistrée qui existeront malgré la mise en place d'une stratégie de communication efficace en urgence et durant toute l'ouverture du sinistre. L'entreprise sinistrée perd des clients, des prospects, des partenaires commerciaux, des contrats en cours de négociation. L'entreprise perd aussi du chiffre d'affaires du fait du dysfonctionnement du système

[25] CENTRE FOR RISK STUDIES, University of Cambridge Judge Business School & Risk Management Solutions (RMS), *2017 Cyber Risk Landscape*, 23 p et 25 p.

d'information qui perdure un certain laps de temps et qui n'aurait pas été rattrapé par mesures permettant de maintenir le niveau d'activité *ante* sinistre.

Les pertes d'exploitation sont comprises chez certains assureurs comme les pertes de revenus et les frais supplémentaires d'exploitation.[26] Les pertes de revenus sont formées par la perte de marge brute d'exploitation directement causée par l'interruption des activités professionnelles consécutive au sinistre. Les frais supplémentaires d'exploitation sont les coûts des mesures correctives mises en place afin d'éviter ou de limiter les conséquences pécuniaires du sinistre et de reprendre le plus rapidement possible les activités professionnelles. Il est donc possible que l'assureur finance la location de matériels informatiques par exemple, le temps que le système d'information soit rétabli. Les frais supplémentaires d'exploitation peuvent consister en la réparation ou le remplacement du système d'information si ces frais sont inférieurs à la perte de marge brute d'exploitation.

Il s'agit d'un poste conséquent d'indemnisation. Cette garantie est donc souvent accompagnée d'une franchise de temps. Il s'agit d'une durée déterminée consécutive à la survenance du sinistre pendant laquelle les pertes d'exploitation restent à la charge de l'assuré, l'assureur prenant la main au seuil de franchise dépassé.

A ce sujet, les attaques par déni de service (DDos) continuent d'être une composante majeure dans le paysage du cyber risque. Le nombre d'attaques DDoS envers les entreprises augmente de 130% d'année en année et l'intensité de ces attaques bat de nouveaux records. L'avènement de l'Internet des objets[27] a permis de mettre en ligne des systèmes avec de faibles niveaux de sécurité. 70% des objets connectés sont vulnérables aux cyberattaques du fait de mots de passe faibles ou d'interfaces web non sécurisées. Ces objets connectés peuvent être la source d'un trafic envers une cible afin de la mettre hors service. Ce type d'attaque va devenir habituel à ce que le nombre d'objets connectés prolifère. Certains secteurs d'activité sont plus fréquemment visés par des attaques DDoS, ainsi presque la moitié des attaques sont dirigées vers des entreprises de *gaming* et leurs serveurs, ensuite des entreprises de média et de divertissement et pour terminer des entreprises Internet et Telecom. En termes d'assurance, la durée de ces attaques est un élément déterminant du coût d'un sinistre cyber, et l'est donc aussi dans le calcul des franchises de pertes d'exploitation. De nombreuses attaques DDoS de

[26] BEAZLEY, Conditions générales Beazley Breach Response, 10 p.
[27] Soit l'extension d'internet aux objets, particulièrement du quotidien tels qu'une voiture, une montre, ou une balance.

forte intensité sont en-dessous du seuil habituel de franchise de huit heures. Les attaques de longue durée et de faible intensité et les attaques répétées jusqu'à mise hors service de la cible sont plus communes. Les attaques de forte intensité et de longue durée seront à prendre en considération par les assureurs à l'avenir au titre de la garantie des pertes d'exploitation, à partir du moment où elles arriveront à dépasser le seuil de franchise et à causer d'importantes pertes financières. A l'heure actuelle, il ne s'agit pas encore d'une caractéristique des attaques DDoS.[28]

b) Les garanties de responsabilité civile

Les garanties de responsabilité civile d'un contrat de cyberassurance sont rattachées à la notion d'atteinte au système d'information et/ou aux données. Dans le cadre de cette étude, nous nous pencherons plus précisément sur l'appréhension par la cyberassurance de la responsabilité civile des sous-traitants et sur l'assurabilité des amendes et des pénalités administratives.

i. La notion d'atteinte au système d'information et/ou aux données

Un contrat de cyberassurance couvre aussi les dommages causés par l'atteinte aux données et au système d'information subis par les tiers et qui fondent une réclamation en réparation.

Les dommages subis par les tiers sont variés, à titre d'exemples : contamination du système d'information par la transmission par l'assuré d'un fichier infecté d'un virus, déni de service du fait de l'inaccessibilité des services de l'assuré.

Les entreprises traitent des données confidentielles et personnelles, déterminées comme telles par un contrat ou par la loi. Une atteinte aux données peut impliquer une violation du droit fondamental au respect de la vie privée et justifier alors une demande en réparation. Les entreprises responsables de traitement de données sont aussi assujetties à des obligations de confidentialité, de transparence et de durée de conservation pénalement, civilement et administrativement sanctionnées par le droit de source européenne.

[28] CENTRE FOR RISK STUDIES, University of Cambridge Judge Business School & Risk Management Solutions (RMS), *2017 Cyber Risk Landscape*, 19-20 p et 22 p.

Sont pris en charge par un contrat de cyberassurance les conséquences pécuniaires et frais de défense résultant de toute réclamation de toute personne pour atteinte à des données personnelles ou confidentielles. Les garanties de responsabilité civile sont aussi déclenchées par toute réclamation de tiers pour atteinte à la sécurité du réseau ou du système d'information.

Il est possible d'obtenir la prise en charge des frais de défense et des dommages et intérêts en cas d'engagement de la responsabilité civile de l'assuré liée au contenu d'un site Internet.

Par exemple, Beazley couvre la responsabilité civile de l'assuré en cas d'atteinte aux données, d'atteinte aux systèmes, en cas de retard ou de défaut de révélation par le souscripteur d'une atteinte, en cas de non-respect d'une charte de protection des données en vigueur. Cet assureur couvre aussi la responsabilité liée au contenu d'un site internet au titre de réclamations relatives à des actes de diffamation, de plagiat, de contrefaçon, d'atteinte au droit au respect de la vie privée ou au droit à l'image, notamment.[29]

Hiscox couvre la responsabilité civile de l'assuré en cas d'atteinte à la sécurité et/ou à la confidentialité des données personnelles mais aussi en raison du contenu publié sur un site Internet ou les médias sociaux. Hiscox couvre aussi l'engagement de la responsabilité civile de l'assuré en cas d'atteinte à des données confidentielles de tiers, en cas de transmission de virus ou d'attaque par déni de service.[30]

Sont parfois pris en charge les conséquences pécuniaires et les frais de défense suite à toute réclamation d'un tiers à l'encontre d'un prestataire ou sous-traitant de l'assuré pour atteinte aux données personnelles et confidentielles. Cela est intéressant et participe d'une bonne appréhension par l'assurance du risque cyber. De nombreuses entreprises externalisent le stockage de leurs données et le Règlement général européen de protection des données à caractère personnel prend en considération le cas du sous-traitant. L'article 24 de ce règlement introduit un principe général de responsabilité à la charge du responsable de traitement relativement à la mise en place de mesures techniques et organisationnelles pour assurer le respecter les principes de licéité, transparence, proportionnalité, et de sécurité du traitement des données. Le responsable de traitement doit examiner périodiquement les

[29] BEAZLEY, Conditions générales Beazley Breach Response.
[30] HISCOX, Conditions générales Data Risks.

mesures prises par le sous-traitant dans le sens de la réglementation. L'article 28 de ce règlement accroît la responsabilité des sous-traitants qui ont l'obligation, tout comme le responsable de traitement, de tenir un registre des traitements et de désigner un *data protection officer* (DPO). Ils sont tenus d'une obligation de conseil auprès du responsable de traitement en matière d'étude d'impact, de sécurité et de contribution aux audits. Le sous-traitant ne peut lui-même sous-traiter l'activité de traitement qu'avec l'accord exprès et préalable du responsable de traitement.[31]

A ce titre, AIG dans le Pack Cyber couvre la responsabilité civile de l'assuré, classiquement en cas d'atteinte aux données personnelles, confidentielles et à la sécurité du réseau, mais aussi en cas d'externalisation et de sous-traitance.[32]

Tokio Marine HCC couvre aussi la responsabilité civile des sous-traitants en cas d'atteinte aux données et/ou aux systèmes d'information, mais de manière plus flexible, puisqu'il n'est pas nécessaire de les lister, et donc, de mettre à jour cette liste à chaque changement de sous-traitance.[33] Répondre efficacement au risque cyber demande en effet d'être malléable tant en souscription qu'en gestion de sinistre, sans pour autant perdre en niveau d'expertise.

De nombreux assureurs se demandent comment assurer le *cloud computing*, à savoir laquelle des responsabilités du responsable de traitement propriétaire des données ou du sous-traitant gardien des données est engagée.[34] Par le *cloud*, les entreprises externalisent majoritairement le stockage de leurs données. Il est aussi important de savoir où sont géographiquement situés les serveurs d'hébergement des données, puisque le transfert de données à caractère personnel en dehors de l'Union européenne est strictement réglementé. Tout transfert de données personnelles hors de l'Union européenne n'est possible que s'il est encadré par des outils garantissant un niveau de protection suffisant et approprié. Il est nécessaire de mettre en place des *Binding Corporate Rules*, des règles d'entreprise contraignantes, consistant en des clauses contractuelles types approuvées par la Commission européenne, des codes de conduite ou des mécanismes de certification. Le *Privacy Shield* est

[31] HISCOX, *Protection des données personnelles, Comprendre le règlement européen*, 2017.
[32] AIG, Conditions générales Pack Cyber 072014, 4 p.
[33] MARGUINAUD, Xavier, Cyber Underwriting Manager chez Tokio Marine HCC, Entretien téléphonique, Août 2017.
[34] ALAU, Ingrid, *Mémoire de recherche, Les cyber-risques dans l'entreprise : enjeux et assurance*, Master 2 Droit des assurances, Institut des Assurances de Lyon, 2013.

le mécanisme selon lequel une entreprise assujettie au droit américain est réputée appliquer un minimum standard de principes de protection de la vie privée. L'adhésion est à renouveler annuellement auprès du Ministère du commerce des Etats-Unis. Seul cet agrément autorise l'entreprise à traiter des données à caractère personnel collectées au sein de l'Union européenne.[35]

Loin de réduire la couverture, et compte tenu des évolutions législatives et réglementaires, l'utilisation de services tels que le *cloud* devrait amener les assureurs cyber à inclure au sein de leurs couvertures le risque d'externalisation, qui est une composante majeure du cyber risque et qui remet en question la notion d'assuré.

Cela fait plus globalement écho à la nature « périls dénommés » du contrat de cyberassurance, qui par défaut ne couvre pas les évolutions technologiques les plus récentes, et nécessite donc un certain entrain d'innovation des assureurs pour répondre de manière constante et efficace aux besoins des assurés.

Enfin, le contrat de cyberassurance contenant des garanties de responsabilité civile, il se trouve dans le champ d'application des actions de groupe. La Loi n°2016-1547 du 18 novembre 2016 de modernisation de la justice ouvre la possibilité d'une action de groupe pour faire cesser le traitement illégal de données à caractère personnel. Il s'agit d'une action en vue de stopper le préjudice subi par des personnes physiques. Cette action de groupe ne possède pour l'instant pas de caractère indemnitaire, il n'y a pas de notion de réparation du préjudice.[36] L'impact financier de l'action de groupe sur le montant de l'engagement de la responsabilité civile de l'assuré sera toutefois à considérer. Nous constatons bien que le principal enjeu en matière de responsabilité civile d'un assuré cyber est l'atteinte aux données à caractère personnel.[37]

ii. La prise en charge incertaine des enquêtes et sanctions administratives

Des garanties de cyberassurance peuvent porter sur les frais d'enquêtes et de sanctions administratives, ainsi que sur les pénalités contractuelles PCI-DSS. La responsabilité civile contractuelle peut être exclue du champ d'application du contrat de cyberassurance. Les

[35] HISCOX, *Protection des données personnelles, Comprendre le règlement européen*, 2017.
[36] MOUNIER, Lucien, souscripteur cyber chez Beazley, Formation cyberassurance, Paris, Juin 2017.
[37] ALAU, Ingrid, *Mémoire de recherche, Les cyber-risques dans l'entreprise : enjeux et assurance*, Master 2 Droit des assurances, Institut des Assurances de Lyon, 2013.

garanties de couverture des frais d'enquêtes et de sanctions administratives sont déclenchées par toute réclamation prenant la forme d'une procédure réglementaire engagée par la Commission Nationale de l'Informatique et des Libertés à l'encontre de l'assuré pour violation de la réglementation protectrice des données personnelles par une atteinte au système d'information et/ou aux données.

La Commission nationale de l'informatique et des libertés est crédibilisée dans son pouvoir de sanction par la nouvelle réglementation européenne de protection des données à caractère personnel puisque l'amende qu'elle peut porter à l'encontre des entreprises n'ayant pas respecté leurs obligations de traitement peut aller de 2% à 4% du CA mondial ou de 10 à 20 millions d'euros, selon lequel de ces montants est le plus important. La Commission nationale de l'informatique et des libertés a un pouvoir d'appréciation et sanctionnera les entreprises qui n'auront par exemple pas mis en place de politique de sécurisation des données et des systèmes d'information, ou qui n'auront pas notifié les personnes concernées. La capacité de la société victime à réagir au sinistre cyber pour le restreindre et pour continuer à assurer la protection des données personnelles est prise en considération par l'autorité compétente dans sa décision de sanctionner. L'intérêt de souscrire une cyberassurance n'en est donc que plus vif.

La volonté de protéger les données à caractère personnel est portée par de nombreux Etats dans le monde. En France, les pouvoirs publics poussent à une mise en conformité avec la nouvelle réglementation européenne au plus rapide. La Commission nationale de l'informatique et des libertés embauche massivement pour avertir et sanctionner. D'autres autorités compétentes européennes ont déjà commencé à condamner les entreprises manquant de diligence dans leurs obligations de protection à hauteur de plusieurs millions. Le règlement européen est déjà appliqué dans certains Etats.[38]

Il est toutefois possible que cette garantie sorte du giron de la cyberassurance pour cause d'inassurabilité, ce qui constitue une limite à la cyberassurance, tout comme cela constitue une limite à l'assurance dans sa globalité.

Par conséquent, les assureurs formulent cette garantie de manière assez évasive, à savoir que les amendes et pénalités administratives sont prises en charge lorsqu'elles sont

[38] AIG, Autopsie d'un sinistre, Risques de cybercriminalité, classe virtuelle, 30 juin 2017.

légalement assurables au regard du droit applicable. Pour ce qui est du droit français, les assureurs résident dans l'attente d'une position plus explicite de la part de la Commission nationale de l'informatique et des libertés, ou in fine, de la jurisprudence sur l'assurabilité de ces amendes.

2 La prévalence de prestations de gestion de crise

Le volet gestion de crise est le fer de lance des contrats de cyberassurance. Associé au mécanisme de transfert financier, il est représentatif de l'aspect innovant des contrats de cyberassurance par rapport aux lignes d'assurance traditionnelles sur le risque cyber.

a) Prestations de dommages d'urgence

Actuellement, ce volet « gestion de crise » est constitué des garanties de dommages activées en urgence, c'est-à-dire que nous y retrouvons toutes les garanties de dommages évoquées précédemment à l'exclusion des pertes d'exploitation et des frais de cyber extorsion. Sont incluses dans le volet gestion de crise les garanties de dommages des frais de recherche de la cause du sinistre et de rétablissement du système d'information, des frais de communication et de relations publiques, de restauration des données et de notification. Ces frais sont complétés par les frais de *monitoring* lorsque des données bancaires sont impliquées.

b) Gestion de crise : de la mise à disposition à la coordination

Ces garanties de dommages sont combinées à des prestations d'assistance et de gestion de crise.

Cette gestion de crise peut être réalisée de plusieurs manières. Pour l'instant, les assureurs concluent souvent des partenariats avec des prestataires de services informatiques, juridiques, de relations publiques et de communication afin de les mettre à disposition de l'assuré.

Le volet gestion de crise du contrat cyber est impératif, car à la survenance d'un sinistre cyber, il faut enquêter, communiquer, endiguer. Une cyberattaque fonctionne par effet domino. Plus l'entreprise réagit vite et bien plus elle a de chance de minimiser le dommage et

de clore rapidement le sinistre. Le positionnement spécifique de l'assureur en tant que gestionnaire de crise est stratégique pour les petites et moyennes entreprises et les particuliers car ces cibles n'ont généralement pas les moyens de réagir vite et bien à un sinistre cyber. Il est tout autant intéressant pour les entreprises grands comptes d'activer leur police cyber lors de la survenance d'un sinistre afin de bénéficier d'un avis extérieur qui permet une prise de recul.[39] Les premières 48 heures en suite au sinistre sont déterminantes. C'est durant ce laps de temps que vont intervenir les mesures phares du volet gestion de crise : les mesures d'urgence. Plus qu'une simple prise en charge de frais, ces garanties dommages combinées à des partenariats de gestion de crise forment une mise à disposition d'un panel d'experts, sans application de franchises.

Hiscox dans son produit Data Risks[40] propose des services d'expertise en sécurité informatique afin d'identifier la faille de sécurité, de préconiser des solutions pour la pallier, d'identifier les auteurs d'une cyberattaque et de constituer un dossier de recours. Un avocat est affecté afin d'identifier la nature et la portée des obligations légales et réglementaires. Un spécialiste en communication a pour mission d'aider l'assuré dans sa communication externe afin de limiter l'impact du sinistre sur sa réputation.

La transparence sur les prestataires de gestion de crise et la qualité de leurs services sont primordiales en ce qu'elles doivent constituer un critère déterminant dans le choix de l'assureur cyber.

Nous pouvons citer Jimaan Sané, Souscripteur Technologies, Médias et Société de services chez Beazley : « (…) *De plus en plus d'acheteurs s'adressent aux assureurs pour qu'ils agissent en fournisseur de services lorsqu'il s'agit de gérer les conséquences d'une violation importante. Le volet services représente, selon nous, un moteur essentiel de croissance des cyber-assurances* ». « *Notre expérience montre que les motivations qui conduisent nos clients à souscrire notre cyber-solution, Beazley Breach Response (BBR), sont de trouver le bon interlocuteur, en cas d'incident, pour se tirer d'affaire, contrôler les pertes et atténuer les risques financiers* ».[41]

[39] AIG, Autopsie d'un sinistre, Risques de cybercriminalité, classe virtuelle, 30 juin 2017.
[40] Produit qui évolue en septembre 2017 pour devenir Cyber Clean.
[41] BICHARD, Jean Philippe, *Beazley : affaire Sony, une jurisprudence ?*, Cyber Risques NEWS, Juillet 2014.

Dans l'idéal, au-delà de la mise à disposition, l'assureur se fait véritable coordinateur de gestion de crise entre les différents experts du panel et avec l'assuré. Cette pratique est encore minoritaire mais gagnerait à se développer.[42] La conclusion de partenariats avec des experts permet à l'assureur de se positionner en tant qu'interlocuteur spécialisé capable d'apporter une réponse rapide et adaptée au sinistre. L'assureur a une vision panoramique du sinistre et globale des sinistres cyber de son portefeuille profitable à l'assuré.

B Distinguer la cyberassurance des lignes d'assurance traditionnelles

Nous présentons le contrat de cyberassurance et les diverses problématiques qui y sont relatives. Dans cette logique, il est intéressant de comparer le contrat de cyberassurance aux lignes traditionnelles d'assurance qui pourraient dans l'éventualité s'appliquer à un sinistre cyber.

Si des lignes spécifiques de cyberassurance sont apparues, elles ne monopolisent néanmoins pas l'assurance du risque cyber, ce qui amène inéluctablement à des éventuels cumuls d'assurances avec les polices traditionnelles et inversement à des absences de garanties sur la globalité du risque cyber. En effet, la plupart des contrats de cyberassurance ne couvrent pas les conséquences matérielles[43] d'une atteinte au système d'information et/ou aux données, comme les polices traditionnelles peuvent explicitement exclure le risque cyber ou certains types de dommage.

1 Sur les conséquences immatérielles d'une atteinte au système d'information et/ou aux données

Les polices spécifiques de cyberassurance sont apparues notamment parce que lignes traditionnelles d'assurance apportent une réponse partielle au cyber risque, ne couvrant que la responsabilité civile ou les dommages ou n'en couvrant pas les conséquences immatérielles

[42] MARGUINAUD, Xavier, Cyber Underwriting Manager chez Tokio Marine HCC, Entretien téléphonique, Août 2017.
[43] Nous comprenons les conséquences matérielles d'un sinistre comme étant matérielles et corporelles.

ou de manière sous-limitée. Ces contrats n'apportent pas de prestations de gestion de crise adaptées au risque cyber, ni d'intermédiaire spécialisé.

a) La cyberassurance et les contrats de responsabilité civile professionnelle et des dirigeants

Le volet responsabilité civile d'un contrat de cyberassurance ne se déclenche pas sur le même fondement qu'un contrat d'assurance de responsabilité civile professionnelle.

Un contrat de responsabilité civile professionnelle ou générale, selon les termes des assureurs, couvre les conséquences pécuniaires et les frais de défense d'une erreur, négligence, omission causant dans le cadre de l'activité professionnelle un dommage à un tiers qui en réclame réparation.

Un contrat couvrant une responsabilité civile professionnelle est liée à la notion de faute, ce qui n'est pas le cas d'un contrat cyber, lié à la notion d'atteinte au système d'information et/ou aux données.[44]

Les garanties de responsabilité civile d'un contrat de cyberassurance sont adaptées au risque cyber. Un contrat d'assurance de responsabilité civile professionnelle, hormis chez les assureurs anglo-saxons, contient une garantie des dommages immatériels non consécutifs souvent très sous-limitée. De plus, le mode d'activation des contrats traditionnels est trop rigide et lent pour être adapté à la prise en charge d'un sinistre cyber, qui demande de la réactivité et de l'efficacité. L'intervention de l'assureur cyber ne peut pas se faire auprès réclamation écrite du tiers.

Une police de responsabilité civile professionnelle face à une intrusion dans le système d'information pourrait éventuellement prendre en charge de manière sous-limitée les frais de défense et les conséquences pécuniaires de cette intrusion. Elle ne couvrirait pas l'atteinte à l'image, les pertes d'exploitation, les frais de restauration, les frais de notification, les enquêtes et les sanctions de la Commission nationale de l'informatique et des libertés, car un contrat de responsabilité civile professionnelle n'est pas un contrat mixte.[45]

[44] PIRSON, Astrid-Marie, Directrice de la souscription Hiscox France, Atelier cybersécurité, Paris, Juin 2017.
[45] AIG, Autopsie d'un sinistre, Risques de cybercriminalité, classe virtuelle, 30 juin 2017.

Une police de responsabilité civile professionnelle ne répondrait donc que très partiellement à la menace cyber. Elle ne couvrirait, dans le champ d'application des contrats de cyberassurance, que la responsabilité civile liée à la protection des données à caractère personnel et la responsabilité civile liée à la sécurité des systèmes d'information,[46] dont l'obligation a été établie pour toute entreprise depuis la Loi Informatique et Libertés de 1978.[47]

La police de responsabilité civile professionnelle conserve néanmoins de l'intérêt sur le risque cyber dans les hypothèses où le risque cyber est indissociable d'un risque de responsabilité civile professionnelle élevé, par exemple, concernant les hébergeurs, le tertiaire informatique, ou le secteur des télécoms. Dans ces configurations, le risque de responsabilité peut être exclu des polices de cyberassurance. Les polices de cyberassurance et de responsabilité civile professionnelle doivent donc être articulées l'une par rapport à l'autre afin d'éviter des trous de garantie. Cela confirme l'intérêt des polices de cyberassurance à être malléables.[48]

Une autre police de responsabilité civile est fondée sur la notion de faute, la police d'assurance de la responsabilité des dirigeants. Elle pourrait éventuellement être activée en cas d'une faute de gestion à la marge du sinistre cyber.[49] Cela serait plausible dans l'hypothèse où l'entreprise n'aurait pas structuré le processus interne de cybersécurité en définissant clairement le rôle de chaque fonction par exemple. De fait, cette police partage aussi le champ d'application des contrats de cyberassurance sur la responsabilité civile liée à la protection des données personnelles et sur la responsabilité civile liée à la sécurité des systèmes d'information. La police de responsabilité des dirigeants peut aussi couvrir les frais d'enquête, d'assistance et de représentation devant des autorités administratives, et donc, devant la Commission nationale de l'informatique et des libertés.[50]

En tout état de cause, la police d'assurance de la responsabilité des dirigeants subirait les mêmes lacunes que la police d'assurance de responsabilité civile professionnelle à ne pas

[46] GRAS SAVOYE, Lignes financières, *Les cyber risques*, Association Nationale des Industries Alimentaires, avril 2015.
[47] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[48] MOUNIER, Lucien, souscripteur cyber chez Beazley, Formation cyberassurance, Paris, Juin 2017.
[49] AIG, Autopsie d'un sinistre, Risques de cybercriminalité, classe virtuelle, 30 juin 2017.
[50] GRAS SAVOYE, Lignes financières, *Les cyber risques*, Association Nationale des Industries Alimentaires, Avril 2015.

couvrir les frais engagés par l'assuré suite au sinistre indépendamment d'une réclamation tierce. Elle ne présente de même pas de prestations de gestion de crise.

L'hypothèse de cumul d'un contrat de cyberassurance se présente avec de nombreuses autres formes d'assurance de responsabilité civile telle que les contrats d'assurance des réclamations liées à l'emploi ou de responsabilité fiduciaire.[51]

b) La cyberassurance et les différents contrats de dommages et fraude

Un contrat d'assurance de dommages vient classiquement couvrir les dommages subis par l'assuré dans l'actif de son patrimoine. Différentes couvertures de dommages traditionnelles peuvent être confrontées à la cyberassurance : l'assurance de dommages aux biens généraliste, l'assurance tous risques informatiques, le contrat dommages immatériels informatiques, et l'assurance fraude.

Les polices dommages échouent tout autant que les polices de responsabilité civile professionnelle à gérer le risque cyber de sa globalité, à supposer que le produit d'assurance de dommages contienne la garantie souvent optionnelle des risques technologiques et prenne en charge des dommages matériels et immatériels. Les garanties de pertes d'exploitation et des frais de reconstitution contenues dans les contrats de dommages traditionnels ne sont généralement pas accordés en cas de dommage immatériel.

Face à un *ransomware*, la police dommages peut toutefois éventuellement couvrir les pertes d'exploitation, les frais supplémentaires d'exploitation, ainsi que les pertes matérielles mais ne prendra pas en charge les frais de consultation cyber, d'extorsion, de décryptage, de reconstitution des données, de notification, de rançon, qui sont des frais spécifiques au domaine cyber.[52] Une police dommages est « listée » et ne prendra pas en couverture un dommage qu'elle n'a pas prévu.

Une assurance tous risques informatiques couvre uniquement les dommages matériels subis par les équipements informatiques, quand bien même sa nature est en « Tous Risques ». Cette assurance intervient suite à un dommage matériel tel qu'un incendie, une explosion, un dégât des eaux ou des dommages électriques. Elle couvre la détérioration, destruction, perte

[51] BENTZ, H., Thomas, *Is your cyber liability insurance any good ? A guide for banks to evaluate their cyber liability insurance coverage*, 2017, 7-8 p.
[52] AIG, Autopsie d'un sinistre, Risques de cybercriminalité, classe virtuelle, 30 juin 2017.

ou vol du matériel informatique et bureautique et du matériel périphérique au sein des locaux assurés, en cours de transport ou chez les tiers. En extension, il est possible de trouver la garantie des frais de reconstitution des informations contenues sur les supports, mais de façon consécutive à un dommage matériel.[53]

Le contrat dommages immatériels informatiques est intéressant en ce qu'il s'applique aux atteintes immatérielles aux données.[54] Il est dans le champ d'application du contrat de cyberassurance mais ne recouvre qu'une partie des conséquences d'une atteinte à des données. Sont pris en charge les frais de reconstitution, de décontamination de virus, d'exploitation, d'identification de la cause du sinistre, les dépenses en relations publiques et en sauvegarde d'image. Une extension extorsion peut être souscrite.

L'assurance fraude couvre le patrimoine financier de l'entreprise à l'encontre des infractions de droit pénal des affaires, comme l'abus de confiance, l'usurpation d'identité, ou l'escroquerie, qui sont commises grâce au moyen de technologies de l'information. L'assurance fraude garantit des valeurs financières alors que la cyberassurance prémunit le système d'information et les données qu'il contient. La police fraude ne recouvre qu'une certaine typologie de risque cyber, le risque cyber impactant des valeurs financières.

L'assurance fraude peut fournir des services de gestion de crise. Généralement, elle contient des garanties dommages des honoraires d'expert (*forensics*, consultants informatiques), les frais de reconstitution des données, les frais supplémentaires d'exploitation ou de décontamination des systèmes d'information. Sur le volet responsabilité civile, elle peut couvrir les conséquences de la transmission d'un virus informatique.[55]

Toutefois, dans l'hypothèse d'un détournement de service par intrusion dans le système d'information, le pirate modifiant les données et profils clients pour détourner des fonds, la police fraude n'intervient qu'après franchises. Elle ne prend pas en charge les pertes d'exploitation, les frais de notification, les réclamations des tiers,[56] les frais d'enquêtes et de sanctions de la Commission nationale de l'informatique et des libertés.[57]

[53] LEYTON, *Libre blanc : les cyber risques*, Juin 2015, 9-10 p.
[54] LEYTON, *supra*.
[55] GRAS SAVOYE, Lignes financières, *Les cyber risques*, Association Nationale des Industries Alimentaires, Avril 2015.
[56] Autres que relatives à la transmission de virus, dans l'hypothèse où cette garantie aurait été souscrite.
[57] AIG, Autopsie d'un sinistre, Risques de cybercriminalité, classe virtuelle, 30 juin 2017.

Il existe des contrats combinés cyber fraude, comme le propose par exemple l'assureur CNA.

c) La cyberassurance et le contrat kidnapping et rançon

Le contrat de cyberassurance se distingue du contrat d'assurance kidnapping et rançon en ce que le risque couvert est différent.

La police kidnapping et rançon face à un *ransomware* pourrait couvrir les frais de rançon, y compris de consultation, ce qu'excluent en général les polices dommages, mais ne prendrait pas en charge les pertes d'exploitation, les frais de consultation cybersécurité, de reconstitution, de notification, d'enquêtes et de sanctions de la Commission nationale de l'informatique et des libertés.[58]

Cela dit, le parallèle reste intéressant car le risque de kidnapping et de rançon demande lui aussi une fine analyse à la souscription et une gestion de crise efficace, avec des mesures d'urgence primordiales. Cette police est aussi l'une des rares à couvrir l'extorsion de fonds, même si cette couverture est généralement sous-limitée.

2 Sur les conséquences matérielles d'une atteinte au système et/ou aux données

Nous avons constaté que le contrat de cyberassurance constituait le seul contrat du marché de l'assurance à apporter une solution adaptée au risque cyber de par sa nature mixte, ses garanties spécifiques, combinées à des prestations de gestion de crise adéquates.

Cela dit, des possibilités de cumul d'assurances existent puisque les lignes traditionnelles d'assurance de dommages et de responsabilité civile professionnelle viennent partiellement couvrir des dommages immatériels consécutifs à un sinistre cyber. Le cumul d'assurances implique des recours en indemnisation entre assureurs à la suite d'un sinistre. Il est nécessaire de déterminer quelle police s'applique en première ligne d'indemnisation et quelles sont les modalités de répartition du montant total de perte entre les assureurs. Le cumul d'assurances entraîne un coût surabondant d'assurance dans le budget de l'assuré.

[58] AIG, *supra*.

Si les contrats des lignes traditionnelles de responsabilité civile professionnelle et de dommages ne prennent pas en charge, ou très partiellement, les conséquences immatérielles d'un sinistre cyber, les contrats de cyberassurance, dans leur globalité, n'en couvriront pas les conséquences matérielles. En effet, les contrats de cyberassurance portent souvent en eux une exclusion des conséquences matérielles consécutives à une atteinte au système d'information et/ou aux données. A priori, la possibilité de cumul d'assurances ne se retrouve donc pas sur les dommages matériels consécutifs à une atteinte au système d'information et/ou aux données.

Néanmoins, nous constatons alors que les contrats de cyberassurance, qui apportent une réponse pourtant adaptée au risque cyber parce que mixte, ne recouvrent pas le risque cyber dans sa globalité. Certains courtiers poussent à la couverture de ces dommages matériels par les programmes autonomes de cyberassurance et il est donc possible de la voir apparaître dans certains contrats, de façon minoritaire. Ces contrats de cyberassurance prennent en charge les dommages matériels consécutifs à une cyberattaque ou un cyber incident. Dans cette hypothèse, la possibilité de cumul entre la cyberassurance et les assurances traditionnelles sur la prise en charge des dits dommages matériels réapparaît. Tous les autres contrats de cyberassurance excluent la prise en charge de ces dommages.

Du fait de cette dernière exclusion de la cyberassurance, les assurés ont cherché une autre manière d'indemniser les dommages matériels d'un sinistre cyber car ces derniers peuvent être conséquents en fonction du secteur d'activité impacté par le sinistre. Les polices traditionnelles qui n'auraient pas exclu ou qui auraient inclus le risque cyber dans leurs conditions générales peuvent alors trouver à s'appliquer aux conséquences matérielles du sinistre cyber, sans pour autant parvenir à y apporter une réponse globale, puisqu'elles n'ont pas de nature mixte.

Les polices traditionnelles qui n'auraient pas exclu le risque cyber de leur champ d'application sans pour autant l'inclure sont dites silencieusement exposées au risque cyber, car leur périmètre d'intervention n'est pas déterminé. En effet, de nombreuses polices d'assurance traditionnelles des lignes professionnelles sont en base « Tous Risques » sans exclure explicitement les pertes consécutives à la réalisation d'un risque cyber.[59] Ces polices

[59] CENTRE FOR RISK STUDIES, University of Cambridge Judge Business School, *Cyber insurance exposure data schema V1.0*, Cyber Accumulation Risk Management, Cambridge Risk Framework, 2015, 6 p.

d'assurance, à la différence de la plupart des polices de cyberassurance, ne contiennent pas d'exclusion relative à la couverture de dommages matériels. Elles peuvent toutefois contenir une exclusion sur les dommages immatériels.

Un contrat de cyberassurance, à l'inverse, constitue une prise en charge affirmative du risque cyber, quand bien même cette dernière en serait limitée aux conséquences immatérielles.

L'éventualité d'une prise en charge silencieuse des conséquences du risque cyber n'est pas à considérer lorsque le risque cyber est soit explicitement couvert, soit exclu.

La nature des dommages pris en charge n'est pas synonyme d'exposition au risque.

Nous pouvons synthétiser l'exposition au risque cyber de l'ensemble des polices d'assurance d'un portefeuille de cette façon :

		Exposition affirmée au risque cyber car couvert	Exposition silencieuse au risque cyber	Pas d'exposition au risque cyber car exclu
Polices d'assurance traditionnelles	Dommages immatériels	Exclusion ou couverture sous-limitée	Exclusion ou couverture	Non garantie
	Dommages matériels	Couverture	Couverture	Non garantie
Polices de cyberassurance	Dommages immatériels	Couverture	N/A	N/A
	Dommages matériels	Exclusion ou couverture	N/A	N/A

Un sinistre cyber peut effectivement causer des dommages matériels. Une atteinte au système d'information et/ou aux données peut causer un incendie, une explosion, un dégât des eaux, des dommages électriques et industriels majeurs. Les cyberattaques présentent un potentiel pour causer des dommages matériels lorsqu'elles visent des systèmes d'information opérationnels ou de contrôle de procédés matériels. Ce type d'attaque peut viser par exemple le fonctionnement d'une centrifugeuse qui sépare de la matière nucléaire, comme l'a fait

l'attaque Stuxnet. L'attaque peut aussi viser un générateur électrique, ou le système autopilote d'un avion.[60]

Une cyberattaque peut donc causer des dommages corporels. Il s'agit par exemple de l'hypothèse de cyber extorsion visant un hôpital. Dans une telle configuration, la vie de certains patients est mise en jeu par la menace de destruction et la mise hors service du système d'information.

Selon les termes traduits de Scott Stransky, Assistant Vice President et ingénieur chez AIR Worldwilde, une entreprise de modélisation de risque, le risque « silencieux silencieux », doublement silencieux, représente le risque élevé dont sont affectées indirectement les polices non cyber par un évènement cyber. Par exemple, en avril 2017, une fréquence radio piratée a déclenché les 156 sirènes d'alarme météo de la ville de Dallas, permettant habituellement de prévenir de l'arrivée d'une tornade. 4 400 appels ont été dirigés au centre d'appel du numéro d'urgence 911 alors en sous-effectif, ce qui a impliqué des retards significatifs de traitement des appels. Le problème induit peut être multiple : à déclencher les sirènes relativement souvent, les habitants finiront par les ignorer, et ce même lorsqu'une tornade aura effectivement été détectée. Des dommages corporels et matériels auraient pu suivre cet événement : des personnes traversant en panique la route et provocant des accidents par exemple. Des magasins alimentaires auraient pu être braqués en prévention d'une éventuelle pénurie.[61]

Ainsi, les cyberattaques peuvent déclencher différentes polices d'assurance selon le système d'information ciblé et les dommages qui en ont résulté. Par exemple, une attaque de la catégorie « technologies de l'information », comme une violation de données, activera certainement le contrat de cyberassurance parce qu'elle provoquera majoritairement des dommages immatériels. Néanmoins, une attaque de la catégorie des « technologies opérationnelles », comme une attaque visant un site industriel, entraînera plutôt l'activation des polices traditionnelles de dommages et de responsabilité civile.[62] L'intérêt de souscrire une cyberassurance couvrant les atteintes relatives aux systèmes d'information industriels est

[60] CENTRE FOR RISK STUDIES, University of Cambridge Judge Business School & Risk Management Solutions (RMS), *2017 Cyber Risk Landscape*, 27 p.
[61] LENIHAN, Rob, *Double trouble with 'silent silent' cyber*, Business Insurance, Juillet 2017.
[62] CENTRE FOR RISK STUDIES, University of Cambridge Judge Business School, *The insurance implications of a cyber attack on the US power grid*, Business Blackout, Society & Security, Emerging Risk Report - 2015 Innovation Series, 25 p.

amoindri par rapport à celui de souscrire une cyberassurance couvrant les atteintes visant les systèmes d'information communs. Le dilemme est tangible, puisqu'il n'est pas certain que les polices traditionnelles d'assurance couvrent les dommages immatériels consécutifs à un sinistre cyber, ni ne prennent en charge des frais spécifiques au risque cyber tels que des frais de notification ou d'expertise technique.[63] Les polices traditionnelles contiennent en majorité une exclusion de couverture des dommages immatériels. Pour l'heure, la cyberassurance est plus adaptée à couvrir des systèmes d'information communs qui attaqués sont moins susceptibles de causer des dommages matériels ou corporels.

Chez les assureurs anglo-saxons, dans les polices de responsabilité civile, sont souvent exclues les réclamations suite à des cyberattaques commises avec malice ou relevant des actes de guerre. Les polices dommages excluent les cyberattaques sauf en cas d'incendie ou d'explosion.[64]

L'absence majoritaire de prise en charge des conséquences matérielles d'un sinistre cyber par les contrats de cyberassurance combinée à un périmètre explicite et prévisible des polices traditionnelles excluant le risque cyber le plus silencieux amènerait à une absence de couverture de ces dommages. La couverture silencieuse des conséquences matérielles du risque cyber par les polices traditionnelles vient pour l'instant combler l'absence de prise en charge de ces dommages dans la majorité des polices spécifiques de cyberassurance. La tendance des assureurs anglo-saxons à exclure le risque cyber des polices traditionnelles expliquerait pourquoi certains courtiers plaident pour la couverture des dommages matériels consécutifs à une atteinte au système d'information et/ou aux données par les polices de cyberassurance.

[63] DESCAZEAUX, Martin, *Assurer son système d'information industriel contre une cyberattaque, c'est possible ?*, Le blog cyber-sécurité des consultants Wavestone, Wavestone Riskinsight, Décembre 2015.
[64] CENTRE FOR RISK STUDIES, University of Cambridge Judge Business School & Risk Management Solutions (RMS), *2017 Cyber Risk Landscape*, 27 p et 29 p.

II Les limites des contrats de cyberassurance

Nous avons constaté que les contrats de cyberassurance présentent une solution novatrice afin de répondre au cyber risque. Cette solution de la cyberassurance est toutefois en construction et n'aboutit pour l'instant pas à prendre en couverture l'ensemble des conséquences de la réalisation d'un risque cyber.

Dans la suite de notre premier développement, nous sommes capables de discerner deux limites aux programmes de cyberassurance.

D'abord, les programmes de cyberassurance font partie d'un processus plus global de maîtrise de risque cyber. Le processus de cyber résilience ne dépend pas seulement de l'assureur. Le contrat de cyberassurance n'est pas, encore, un contrat de gestion de risque. Les programmes de cyberassurance s'inscrivent dans un panorama plus global de gouvernance impliquant des décisions managériales, techniques, comportementales, gouvernementales. L'assureur peut dynamiser le processus de cyber résilience et pleinement y contribuer en persévérant dans l'innovation de son métier. La gouvernance de risque cyber transcende les limites de l'assurance et pour l'heure, de la cyberassurance aussi.

Ensuite, les programmes de cyberassurance se heurtent à leurs propres limites assurantielles. Le risque cyber est complexe et demande d'être souscrit différemment que de façon traditionnelle. Le risque cyber est aussi un risque protéiforme capable d'impacter de façon catastrophique le portefeuille cyber et le portefeuille global d'un assureur d'une capacité maximale difficile à modéliser et à matérialiser en amont. L'assureur cyber est confronté à une importante problématique d'accumulation de risque cyber qui pour l'heure n'est pas encore solutionnée. Cette problématique amène les assureurs à développer des programmes de réassurance et à questionner la réassurance publique, lorsque le risque cyber se fait inassurable.

A La cyberassurance confrontée à la cyber résilience

Le contrat de cyberassurance n'est pour l'instant pas un contrat de gestion de risque.

De fait, des mesures de cyber résilience doivent l'encadrer pour permettre une gestion efficace de risque cyber et *in fine* profitable au marché de la cyberassurance. L'assureur cyber à un rôle d'incitation à jouer dans la mise en œuvre de mesures globales de cyber résilience. Il s'agit de favoriser la collaboration entre acteurs de la cyber résilience mais aussi entre assureurs cyber, d'impliquer les pouvoirs publics dans la sensibilisation au risque cyber et de contribuer à la responsabilisation des assurés.

L'assureur cyber peut aussi dynamiser le processus de cyber résilience en améliorant la cyberassurance et innover la gestion de crise en gestion de risque. Alors l'assureur se positionne en véritable clé de voute du processus de cyber résilience. Il se trouve en effet à une place décisive pour devenir un véritable gestionnaire de risque.

1 Collaborer avec les acteurs de la cyber résilience

L'assureur peut dynamiser le processus de cyber résilience en développant des partenariats de collaboration. La participation des pouvoirs publics dans la sensibilisation au risque cyber est de même plébiscitée.

a) Entre assurance et technique : la création d'un référentiel commun

Appréhender le risque cyber demande la collaboration de multiples acteurs pluridisciplinaires impliqués dans le processus de cyber résilience, dont le domaine d'expertise va de la technique au juridique en passant par les relations publiques et le management de risque. Ces différents acteurs ne partagent pas le même langage et cela nuit à la lisibilité des offres d'assurance, à leur mise en place, à leur gestion et plus globalement, au processus de cyber résilience. La cybersécurité est gouvernée par la multiplicité des standards. Il serait intéressant d'élaborer un référentiel commun contenant des définitions communes des risques et des méthodes de protection, ainsi que des contenus traités informatiquement. Ce

référentiel est à actualiser au fur et à mesure du progrès technologique, des menaces et des attaques.[65] Il permettrait notamment de vulgariser le savoir technique auprès des assureurs.

Cette méthode trouverait par exemple son utilité pour définir le *cloud* et performer sa couverture d'assurance, ce qui n'est pas forcément le cas pour l'instant alors que de nombreux assurés y recourent.

Comme évoqué, le risque cyber est aussi un risque managérial et comportemental. Une police d'assurance cyber sera inefficace si elle n'est pas accompagnée d'une prise de conscience des dirigeants, responsables cybersécurité, responsables juridiques, sous-traitants, clients, particuliers et pouvoirs publics. Il faut présenter le risque cyber comme un risque d'entreprise auprès des professionnels[66], comme un risque de la vie courante auprès des particuliers, comme un risque de la vie économique pour les Etats. Il faut comprendre l'impact du risque, et ne pas se focaliser uniquement sur la technique de l'attaque, ou la prise en charge financière de ses conséquences. Il est réducteur de considérer exclusivement le risque cyber par le prisme de sa technicité.[67]

L'élaboration de ce référentiel commun devrait toutefois se cantonner aux fondamentaux et aux tendances émergentes, car une mise en commun précoce sur des risques cyber nouveaux pourrait nuire à leur compréhension et à l'innovation dans les divers métiers de la cyber résilience.

b) Intra-assurance : standardisation controversée et partage de données sinistre

La nécessité de mutualiser et standardiser les méthodes concerne aussi le milieu intra-assurance spécialisé sur le risque cyber. Certains énoncent qu'il serait intéressant que le marché de la cyberassurance progresse en standardisant les garanties et termes des conditions générales d'assurance. Cela participerait bien sûr d'une meilleure lisibilité des offres. Souscrire un contrat de cyberassurance est un challenge pour l'assuré, qui peine à comparer les offres afin de cerner lequel de ces contrats lui serait le plus adapté.

---

[65] TELECOM ParisTech, Alumni, *Livre blanc : comment « débloquer » le marché de l'assurance cyber en France ?*, Juin 2017, 11 p et 14 p.
[66] TELECOM ParisTech, Alumni, *Livre blanc : comment « débloquer » le marché de l'assurance cyber en France ?*, Juin 2017, 16 p.
[67] MARGUINAUD, Xavier, Cyber Underwriting Manager chez Tokio Marine HCC, Entretien téléphonique, Août 2017.

Le risque cyber est néanmoins un risque complexe aux multiples facettes et n'est pas encore maîtrisé par le secteur des assurances. La standardisation peut à l'inverse constituer une limite aux progrès d'appréhension de ce risque par l'assurance. En toute hypothèse, la standardisation devra se limiter aux définitions fondamentales, sans impacter les différentes structures et approches de couverture ou les garanties en elles-mêmes proposées sur ce marché en forte innovation. L'exigence d'adaptation et de renouvellement constant des polices de cyberassurance est antinomique au mécanisme traditionnel de normalisation des garanties. Plus de cinquante assureurs se positionnent sur une ligne spécifique de cyberassurance, et chaque approche est différente. Cette diversité des programmes de cyberassurance est une force du marché. Le mécanisme de standardisation des contrats d'assurance peut venir contrecarrer une gestion adéquate du risque cyber qui nécessite une forte adaptation de l'offre d'assurance au profil de gouvernance, technique et contractuel de l'assuré, à la souscription mais aussi en cours de vie du contrat. Nous remarquons plus d'une fois que le risque cyber est difficilement pris en charge par les mécanismes assurantiels traditionnels. L'intervention du courtier averti afin d'accompagner le prospect dans la phase de souscription mais aussi en cours de vie du contrat est certainement décisive.

Il est de même possible, dans cette variété d'offres bienvenue, d'imaginer un partage de données sinistre entre les assureurs du marché afin que ces derniers progressent en analyse et parviennent à modéliser le risque cyber avec moins de difficulté. Pourrait être créée une base de données des sinistres afin de permettre un environnement sécurisé qui facilite l'échange d'informations anonymisées et donc la maîtrise de risque. Une coopération avec l'Agence nationale de la sécurité des systèmes d'information est ici envisageable[68]. Le risque cyber peut encore être qualifié d'émergent et est en toute hypothèse évolutif et protéiforme. Les assureurs, qu'ils bénéficient ou non d'une expérience de souscription sur plusieurs années[69], n'en ont pas une connaissance technique et statistique absolue et immuable. Cette connaissance imparfaite du risque rend l'appréhension de ses potentiels d'intensité et de fréquence difficile. Le coût d'un sinistre cyber est difficilement quantifiable.

Ce partage d'informations peut être limité à certains types de données. L'essentiel est que la vue panoramique de l'assureur sur les sinistres cyber soit maximisée et qu'il puisse

[68] ASSOCIATION DES PROFESSIONNELS DE LA REASSURANCE EN FRANCE, *Etude sur les « cyber risques » et leur (ré)assurance*, Juin 2016, 39 p.
[69] Les assureurs anglo-saxons aux Etats-Unis.

profiter de toute l'expérience cyber, non pas uniquement sur son portefeuille, mais sur tous les portefeuilles cyber et *in fine* impactés par le risque cyber, afin d'offrir à son assuré la meilleure prestation de gestion de risque. Il s'agit là d'une mesure vertueuse, puisque le risque cyber présente un réel potentiel catastrophique.

c) Impliquer les pouvoirs publics dans la sensibilisation à la cybersécurité

Les pouvoirs publics et les organisations nationales et internationales ont un rôle à jouer dans cette prise de conscience globale relative à la cybersécurité. Ils peuvent être à la source de campagnes de sensibilisation ciblées sur les bonnes pratiques de cybersécurité et mettre en place des plateformes d'alerte, de partage d'informations, mais aussi de gestion de crise. Un service minimum de gestion de crise pourrait être organisé en cas de sinistre cyber catastrophique, ou à défaut d'assurance. La lutte contre les paradis numériques peut aussi devenir un objectif gouvernemental. Des partenariats entre les assureurs privés et certaines émanations publiques pourraient être à la source de formations destinées à des publics novices tels que les particuliers.

Le secteur privé investit aussi dans le processus global de cyber résilience. De nombreuses entreprises financent d'ores et déjà l'implémentation de systèmes de cybersécurité pour protéger leurs valeurs. Cet investissement global croît de 14% par année, passant de 75 milliards de dollars américains en 2015 à 86 en 2016. Ce chiffre devrait dépasser les 100 milliards à la fin de la décennie. En moyenne, les entreprises américaines consacrent 3% de leur budget à la cybersécurité. Ces dépenses sont notamment affectées à la formation et à la sécurisation des objets connectés qui par ailleurs constituent un enjeu pour la cyberassurance à plus d'un titre.

Cet investissement technique doit participer d'une prise de conscience cyber dans l'ensemble des sphères de la société et dans tout type d'activité.

Les pouvoirs publics sont impliqués dans la cyber défense mais gagneraient à être plus impliqués dans le processus de cyber résilience. En mars 2016, le gouvernement du Royaume-Uni a établi un nouveau centre national de cybersécurité. Ce centre a pour mission une cyber défense active, c'est-à-dire hacker en retour les hackers. En avril 2016, le gouvernement allemand a créé une nouvelle direction cyber et information au sein de la *Bundeswerh*

militaire.[70] En France, il a été annoncé que l'Agence nationale de la sécurité des systèmes d'information va mettre en place une plateforme d'assistance aux victimes de cyber malveillance. Il serait intéressant d'impliquer les cyber assureurs dans ce projet. Les Etats doivent démontrer plus d'initiative, ou favoriser l'initiative sur le processus de cyber résilience, et notamment en matière de formation et de prévention du risque cyber. En 2012, Paul Ash a créé en Nouvelle-Zélande le *National Cyber Policy Office* (NCPO) afin de sensibiliser le secteur public, le secteur privé et les individus à la cybersécurité. Le NCPO promeut la coopération entre ces différents acteurs, dont les assureurs font partie, et avise le gouvernement néozélandais en matière de cybersécurité. Il s'agit d'une belle initiative de cyber résilience.[71]

2 Responsabiliser les assurés

Les violations de données à caractère personnel restent majoritairement localisées aux Etats-Unis mais nombreuses d'entre elles ont été rapportées par d'autres Etats en 2016. Les entreprises se responsabilisent partout dans le monde en dévoilant publiquement la violation et en notifiant les personnes affectées, bien que la réglementation applicable en matière de notification ne soit possiblement pas encore aussi élaborée qu'aux Etats-Unis.[72]

Le facteur humain est essentiel au fonctionnement du système d'information. Des salariés utilisent et contrôlent le système d'information quotidiennement. Les fournisseurs de prestations de services informatiques interviennent dans la gestion du système. Ce potentiel humain doit être formé à la cyber résilience.

De même, l'entreprise est plus ou moins vulnérable selon les choix qu'elle effectue en matière de cybersécurité. L'assureur cyber résilient incitera l'assuré à s'équiper selon un minimum ou un certain standard de cybersécurité mais aussi à établir une gouvernance et des procédures de gestion de risque internes efficaces.

L'assureur peut jouer un rôle dans ce processus de responsabilisation des assurés qui pour l'instant n'est pas sous son entière maîtrise, à ce qu'il n'est pas gestionnaire de risque.

[70] CENTRE FOR RISK STUDIES, University of Cambridge Judge Business School & Risk Management Solutions (RMS), *2017 Cyber Risk Landscape*, 7 p et 10 p.
[71] MARGUINAUD, Xavier, Cyber Underwriting Manager chez Tokio Marine HCC, Entretien téléphonique, Août 2017.
[72] CENTRE FOR RISK STUDIES, University of Cambridge Judge Business School & Risk Management Solutions (RMS), *2017 Cyber Risk Landscape*, 15 p.

a) Par l'élaboration de clauses d'exclusion

Un des effets pervers d'un transfert de risque réussi auprès de l'assureur est la déresponsabilisation de l'assuré. La cyberassurance telle qu'elle est configurée aujourd'hui n'est toutefois qu'une composante de la gestion résiliente du risque cyber. L'assuré doit rester diligent et proactif dans la sécurisation de son activité car la législation européenne et mondiale ne cesse de le responsabiliser.

Nous avons à ce sujet constaté que les garanties de responsabilité civile contenues dans le contrat de cyberassurance ne sont pas rattachées à la notion de faute. De même, les volets dommages prennent en charge les frais de notification et il est possible que les amendes administratives soient couvertes. Cela va à l'encontre de la logique législative et réglementaire de renforcement des obligations de l'assuré en matière de cybersécurité. L'assuré, rassuré par la prise en charge financière des conséquences d'un éventuel sinistre, peut manquer de s'investir dans le processus de cyber résilience et spécifiquement de cybersécurité.

La cyberassurance prend le contrepied de cet effet pervers en élaborant des clauses d'exclusion relatives à toute défaillance de l'assuré dans les mesures de sauvegarde ou de cybersécurité. Là encore, il est intéressant de considérer les hypothèses de sous-traitance et d'externalisation de l'activité, puisque ces dernières ont vocation à entrer dans le champ de couverture de la cyberassurance du responsable de traitement ou, plus globalement, du client de ces services. Des exceptions à cette prise en charge pourraient prendre la forme d'exclusions, en cas de non-respect par le sous-traitant des obligations légales ou contractuelles.

b) Par la formation

La formation de l'assuré en matière de cybersécurité est devenue un prérequis impératif. Cette formation n'est pas encore d'initiative publique, mais pourrait l'être. Elle doit donc provenir de l'assuré ou de l'assureur. Un exemple d'implication de l'assureur, et de son intérêt à participer d'ores et déjà à la gestion de risque, est apporté par Hiscox. Cet assureur a développé sur son nouveau produit Cyber Clean une incitation de l'assuré à renforcer ses mesures de cybersécurité en souscrivant le contrat de cyberassurance. Une réduction de prime

est accordée si l'assuré souscrit à la formation continue de cybersécurité SecureSphere créée par EPITA, une école d'ingénieurs en informatique. Cette formation porte sur les fondamentaux de cybersécurité et les bonnes pratiques à adopter en entreprise. De cette façon, l'assuré connaît les mécanismes basiques de la cybersécurité et sera à même d'avoir les bons réflexes, impératifs, en cas de sinistre alors de probabilité réduite. Cette formation technique intervient en phase de souscription. Elle pourrait être accompagnée d'audits de routine à déterminer selon le profil de l'assuré. Une formation continue est une bonne réponse face à un risque évolutif. Elle permet de recycler les savoirs techniques.

Actuellement, la montée d'investissements privés en cybersécurité et les mesures de routine prévenant une perte accidentelle de données par les salariés réduisent effectivement l'incidence des cyberattaques de fréquence et de relativement faible amplitude. Former l'ensemble des acteurs remonte le niveau d'exigence d'un cran envers la cybercriminalité, qui doit faire preuve de plus de talent et de malice pour réussir ses entreprises. De nombreuses cyberattaques visant les entreprises impliquent des salariés. Les hackers déterminés et disposant des moyens adéquats prennent aisément un pas d'avance afin de sauter les barrières de cybersécurité.[73] Il est donc important de définir le processus interne de réponse à une cyberattaque bien avant la survenance du sinistre et même la souscription d'un contrat de cyberassurance, bien que cette dernière contribue à cette définition indéniablement.

Une formation technique reste toutefois insuffisante à accomplir la maîtrise du risque cyber puisque ce dernier ne dépend pas uniquement de facteurs techniques. Cette formation doit être accompagnée de consultations d'expertise en vue d'établir ou d'améliorer le processus de gestion de risque cyber au sein de la structure assurée.

L'assureur a aujourd'hui des possibilités d'influencer positivement les assurés et d'être impliqué dans le processus de cybersécurité mais aussi de cyber résilience. En la matière, il doit être fait du facteur humain un bouclier plutôt qu'une brèche.[74]

[73] CENTRE FOR RISK STUDIES, University of Cambridge Judge Business School & Risk Management Solutions (RMS), *2017 Cyber Risk Landscape*, 8 p et 14 p.
[74] PIRSON, Astrid-Marie, Directrice de la souscription Hiscox France, Atelier cybersécurité, Paris, Juin 2017.

c) *Par l'établissement et l'amélioration de procédures internes de gestion de risque*

La notion de cyber résilience est à opposer à celle de cyberdépendance. Il est nécessaire d'aboutir à une organisation efficace et pertinente des facteurs humains en parallèle des investissements techniques et de conformité effectués. Le niveau d'information et de transparence doit être élevé, les mises à jour fréquentes.

Le *risk manager* ou le *chief risk officer* a un rôle à jouer dans l'entreprise afin de promouvoir la notion de cyber résilience. De ce fait il doit participer à la vie de la cyberassurance de l'entreprise. La cyberassurance est cependant un sujet de direction[75] parce qu'elle fait partie d'un processus global impactant l'organisation interne de la structure assurée, et dépend d'une vue d'ensemble sur les aspects techniques, juridiques, et humains du risque. Les responsables du système d'information ne sont pas toujours enclins à participer à la souscription d'une cyberassurance dont l'achat est confié à la direction des achats et au *risk manager*. Leur rôle est pourtant déterminant dans la connaissance des failles potentielles du système d'information qu'il peut être difficile de reconnaître. Lors d'une crise, le processus d'alerte et d'endiguement d'un sinistre cyber dépend aussi d'une organisation interne efficace. Il est impératif que l'assureur réunisse ces différentes entités et établisse un état de lieu de la cybersécurité et de la cyber résilience dans l'entreprise prospectée ou assurée, tout en proposant des solutions d'amélioration si pertinent.

En complémentarité de la méthode d'exclusion de risque, la cyberassurance peut aussi avoir un rôle à jouer dans la sécurisation des partenariats concernant le traitement des données, ou de vente et d'achat de produits technologiques. De nouvelles pratiques pourraient naître comme la demande d'attestation de cyberassurance systématique et réciproque de l'assuré envers ses prestataires et sous-traitants. L'assureur peut exiger la présence de clauses types dans les contrats de partenariat car ces derniers peuvent influencer la gouvernance du risque cyber.

[75] MARGUINAUD, Xavier, Cyber Underwriting Manager chez Tokio Marine HCC, Entretien téléphonique, Août 2017.

3 Innover la gestion de crise

Cette capacité d'impulsion que l'assureur peut démontrer sur l'ensemble du processus de cyber résilience révèle qu'il est en capacité d'innover la gestion de crise en véritable gestion de risque.

Le contrat de cyberassurance est actuellement centré sur les mesures d'urgence en cas de survenance d'un sinistre et sur la prestation de mise à disposition d'experts. Peu de place est accordée à la prévention, la compréhension du risque, et la correction post-sinistre. Faire de l'assureur un gestionnaire de risque, et non pas seulement de crise, c'est donné pleinement place à l'assurance dans le processus de cybersécurité et de prise de conscience globale. L'assureur peut prendre la main sur les différentes mesures de cyber résilience précédemment développées, de par son expertise des sinistres cyber et sa position centrale entre tous les acteurs de la cyber résilience et panoramique sur le risque cyber. Cantonner l'assureur à son rôle traditionnel de support financier et/ou d'intermédiation avec des experts n'est pas adapté au marché de la cyberassurance, qui permet et nécessite que l'assureur ait la maîtrise du risque. La complexité des sinistres cyber et leur difficile appréhension par la technique et l'assurance démontre tout l'intérêt d'agir en amont et en aval de la réalisation du risque. L'assureur cyber peut contribuer à réduire les coûts et anticiper, prévenir le sinistre cyber et faire en sorte qu'il ne se reproduise pas. Pour l'heure, l'analyse des conséquences d'un sinistre cyber et la quantification de ce dernier sont encore perfectibles mais avec l'expérience, l'assureur deviendra un expert en gestion de risque. Il faut alors lui donner les moyens de participer au montage de la cybersécurité et de la cyber résilience au sein de la structure assurée.

La confortation de l'assureur dans un rôle novateur de gestionnaire de risque permettrait d'améliorer l'efficacité des polices de cyberassurance pour en faire de véritables outils de maîtrise de risque. La mauvaise maîtrise ou l'absence de maîtrise du risque cyber remet en cause la pérennité du marché de la cyberassurance et de la souscription cyber dans sa globalité.

a) Gestion de risque : la coordination préventive et corrective

Le cyber assureur se positionnera comme un gestionnaire de risque, c'est-à-dire en intervenant avant et après sinistre dans un véritable processus de cyber résilience. Cette intervention en vue de prévenir et de corriger un sinistre cyber, qui de toute manière se réalisera, n'est pas commune aux assureurs traditionnels, établis dans un rôle indemnitaire, sans implication dans l'amélioration de la situation de l'assuré. L'assurance traditionnelle n'a pas pour logique d'enrichir l'assuré. Pourtant, face au sinistre cyber, enrichir l'assuré permettrait la création d'un cercle vertueux : un assuré renforcé subit moins de sinistres, ce qui apporte tout autant à l'assureur qui est alors en position de donner de meilleures garanties.[76] La gestion *post-event* est donc tout autant vitale au processus de cyber résilience à ce qu'elle ne doit pas se limiter à la remise de l'assuré à son état *quo ante* mais plutôt à le renforcer. L'assureur gestionnaire de risque doit permettre la compréhension du sinistre et aboutir à des solutions pour ne plus qu'il se reproduise.

Comme évoqué, chez Beazley, l'expert informatique détermine la cause et l'étendue du sinistre cyber, mais il est aussi mis à disposition par l'assureur, qui le reconnaît pour ses prestations de qualité et qui peut même l'avoir formé sur le processus assurantiel de gestion de sinistre. Plus en avant, cet expert informatique pourrait intervenir en souscription de contrat et préconiser de bonnes pratiques de cybersécurité à mettre en place. Il pourrait intervenir *post-event* en prodiguant des conseils d'amélioration de procédures de cybersécurité internes au regard du sinistre. Il est déjà prévu dans les conditions générales de Beazley que cet expert analyse la capacité de l'assuré à éviter un futur incident. Beazley exclut néanmoins de sa couverture les frais d'amélioration des systèmes informatiques.[77]

Cet expert doit travailler avec d'autres experts notamment en management de risque afin d'amener dans toutes les hypothèses le sujet cyber au *board* des décisions.

Nous pouvons reprendre l'exemple concret du module de formation créé par Hiscox et EPITA et imaginer un volet de formation technique intégré au contrat de cyberassurance. Ce dernier serait personnalisé à la cible et mis à jour de façon régulière, avec des audits de

[76] MARGUINAUD, Xavier, Cyber Underwriting Manager chez Tokio Marine HCC, Entretien téléphonique, Août 2017.
[77] BEAZLEY, Conditions générales Beazley Breach Response, 21 p.

routine à programmer selon l'évolution de l'entreprise et l'utilisation qu'elle fait des nouvelles technologies.

Nous avons développé que l'assureur présente les capacités pour devenir la pierre angulaire du processus de cyber résilience. Il possède de nombreuses données pour ce faire, concernant un client mais aussi concernant tout son portefeuille cyber, et, si les assureurs collaborent entre eux, sur l'ensemble des sinistres cyber des assurés. Par sa vision d'ensemble, l'assureur peut coordonner les différents acteurs intervenant sur un sinistre mais aussi lors de la mise en place et durant la vie d'un contrat cyber. Il peut orchestrer la gestion de risque en intervenant de façon préventive et de façon corrective. Plus qu'indemniser l'assuré et lui permettre de revenir à une situation *ante* sinistre, plus que de mettre à disposition de l'assuré des experts certes réactifs et adaptés, l'assureur transcende les principes de l'assurance et vient améliorer la situation de l'assuré.

Dans cette logique de gouvernance du risque cyber, pourquoi ne pas envisager l'émergence d'un contrat cadre de prestation de services de cyber résilience dont l'assurance, entendue de manière traditionnelle, ce serait qu'un volet ? Cette structure cadre serait un véritable outil contractuel de *risk management* donc l'assureur serait le porteur et le coordinateur des différents volets (techniques, juridiques, communication). Dans cette hypothèse de gestion de risque, tous les acteurs sont reliés les uns avec les autres et non pas seulement vers l'assureur ou l'assuré. Il est alors possible de voir émerger dans cette structure des prestations de services combinées entre ces domaines de spécialité. L'assureur pourrait bénéficier de délégations de pouvoir ou de mandats pour diriger l'ensemble de la structure, qui en retour bénéficierait des données sinistre, sous une confidentialité contractuelle et technique. L'Agence nationale de la sécurité des systèmes d'information pourrait tenir un rôle au sein de ce contrat cadre en fixant des mesures de cybersécurité fondamentales à la souscription d'une cyberassurance et en exerçant un contrôle sur leur mise en pratique.[78] Le mécanisme de ce contrat cadre de gestion de risque dépasserait la finalité traditionnelle du mécanisme assurantiel.

[78] Idée de partenariat avec l'Agence nationale de la sécurité des systèmes d'information issue de SCHNEIDER, Laure, *Article Cyber-risques et cyber-assurances*, Banque & Stratégie n°336, ENASS Papers 9, Mai 2015.

b) *Gestion de risque : l'internalisation*

Enfin, il est possible d'envisager plus que de la coordination de gestion de risque. L'assureur peut lui-même prendre la main sur la gestion de risque et internaliser ces prestations.

Nous avons traité des problèmes de dialogue et d'incompréhension possibles entre le secteur des technologies de l'information et le secteur des assurances, et nous traiterons plus en aval du problème de confidentialité soulevé par l'activité de souscription d'une assurance cyber. Ces problèmes peuvent être exacerbés lorsque l'assureur tient un rôle de coordinateur de gestion de risque ou lorsqu'il se contente de mettre à disposition des experts. Il est souvent question de savoir, afin d'apprécier la qualité de service d'un assureur, s'il externalise son service de gestion des sinistres. Pourquoi, à terme, ne pas envisager l'internalisation par les assureurs spécialisés sur le cyber des services techniques, juridiques et de relations publiques permettant de bien gérer un sinistre cyber, et même, de bien gérer le risque cyber ? Ces services seraient capables d'accompagner le client avant la souscription, pendant la vie du contrat, pendant le sinistre en urgence, et *post-event*, en vue de comprendre le sinistre et surtout de faire en sorte que ce sinistre ne se reproduise pas, et donc, d'améliorer la situation de l'assuré. L'assureur dépasse le transfert financier de risque, la gestion de crise, la gestion de risque coordonnée, il est gestionnaire de risque.

Cela demanderait un centre de gestion multilingue et expert des différentes législations dans le monde, ce qui bien sûr expose l'assureur à un coût considérable.[79] Néanmoins, cela présenterait de nombreux avantages. Une innovation accélérée des contrats de cyberassurance serait facilitée, permettant tout autant au marché de la cyberassurance de monter en expertise et en spécialisation que de suivre les mutations technologiques du risque, et qui sait, les devancer peut-être.

Hélas, tout n'est pas si simple et la centralisation de données client implique un risque aggravé de fuite de données, et donc, entre autres, de confidentialité. De même, la somme de données fournies par l'assuré à la souscription ne sera pas gérée par le même service au

[79] MARGUINAUD, Xavier, Cyber Underwriting Manager chez Tokio Marine HCC, Entretien téléphonique, Août 2017.

sinistre. Cela peut aussi être source d'incompréhension entre l'assureur et l'assuré, amener à une rupture de confiance ainsi qu'à une absence d'optimisation de la gestion de risque cyber.

B La cyberassurance confrontée à l'assurance

Nous avons développé les limites qu'atteint la cyberassurance à mettre en pratique la cyber résilience, pourtant intrinsèque à la maîtrise du risque cyber. L'assureur présente toutefois le potentiel pour dynamiser la cyber résilience.

Ce dernier doit aussi faire preuve d'innovation dans son champ traditionnel d'action qu'est l'assurance pour appréhender un risque complexe. Le cyber assureur doit repenser l'activité de souscription et persévérer dans la spécialisation des contrats de cyberassurance en s'adaptant aux divers profils des assurés, par secteur d'activité mais aussi au-delà de la sphère professionnelle.

Le risque cyber est un risque systémique et potentiellement catastrophique. Il interroge la capacité des assureurs, que ce soit sur le portefeuille cyber ou sur le portefeuille global, comme nous l'avons discerné lors de l'étude de l'exposition silencieuse des polices d'assurance traditionnelles au risque cyber. L'assureur cyber est confronté à une véritable problématique d'accumulation de risque cyber et vient limiter par prudence les capacités accordées sur ce risque en première ligne. L'assureur en première ligne peut aujourd'hui mais positionnera plus de capacité demain sur le risque cyber, à mesure de l'amélioration des mécanismes de modélisation du risque cyber et de l'appréhension de ce dernier par l'assurance. Les réassureurs sont pour leur part plus exposés au risque cyber et donc au risque d'insolvabilité sous-jacent car ils financent plusieurs portefeuilles et lignes d'assurance.[80] Manager l'accumulation du risque cyber est un impératif.

Une réassurance publique est parfois sollicitée. Elle l'est tout autant lorsque nous constatons que l'implication des Etats en matière de cyber défense se retrouve parallèlement en matière de cyber attaque, et amène à reconsidérer l'assurabilité du risque cyber par l'assurance privée.

[80] VEZIO, Philippe, Managing Director chez Tokio Marine HCC, entretien téléphonique, Août 2017.

1 Souscrire différemment la cyberassurance

La nature complexe du risque cyber et sa difficile appréhension par les mécanismes traditionnels de l'assurance nécessitent d'innover la souscription de la cyberassurance. La nature malléable de la cyberassurance doit de même être maximisée en adaptant la couverture aux divers secteurs d'activité, qui sont impactés différemment par le risque cyber. Enfin, ce même impératif demande de développer des offres de cyberassurance pour les besoins des particuliers.

a) Approcher le risque cyber avec nouveauté

Approcher le risque cyber avec nouveauté implique de remettre en question les modes de souscription traditionnels de l'assurance tout en portant la réflexion sur la confidentialité de la période précontractuelle, décisive en matière de cyberassurance, mais aussi en cours de contrat.

i. L'entretien et l'audit de souscription

L'appréhension du risque cyber est complexe de par sa technicité, sa constante évolution, sa compréhension variable selon les différents acteurs impliqués dans la cybersécurité et la difficile estimation des pertes dans le cadre de la gestion des sinistres.

Renforcer l'assureur dans son rôle de gestionnaire de risque suppose qu'il bénéfice d'une pleine connaissance du risque et de l'approcher différemment que par la méthode traditionnelle du questionnaire de souscription, avant même toute conclusion de contrat. Trop souvent, la souscription se limite à un questionnaire, et ce particulièrement sur les segments de cible inférieurs. Ce n'est pas un mode adapté de souscription pour le risque cyber. Un questionnaire qui aborde un risque complexe fera une dizaine de pages sans pour autant parvenir à le cerner dans sa globalité. Il se limite souvent à l'aspect technique du risque cyber, à savoir quels équipements sont utilisés par l'assuré, quelles méthodes de sécurité des systèmes sont mises en œuvre, sans pour autant cerner l'entière problématique. L'aspect technique doit être pris en compte, mais pas seulement, car c'est négliger le facteur humain. La rédaction du questionnaire cyber est souvent vécue par les assurés comme une épreuve

longue, fastidieuse et inintelligible. Elle est alors reléguée ou sous-estimée dans son importance, ce qui nuit à l'adaptabilité du contrat aux besoins du client.

De même, les modes de souscription simplifiés tels que la pré-cotation ou la cotation en ligne ne semblent pas pertinents si l'ensemble des acteurs du marché souhaitent monter en expertise. Cela peut de façon superficielle donner une idée de couverture à l'assuré mais ne représente qu'une étape dans un processus de souscription. Ces modes de souscription ne semblent pas adaptés au risque cyber même s'ils s'adressent aux segments les plus petits, car les petites et moyennes entreprises sont tout autant visées par des cyberattaques. Ces cibles sont vulnérables car elles peuvent ne pas avoir mis en place des mesures de cybersécurité assez fiables et ne pas avoir établi une gouvernance de risque. L'interconnectivité des systèmes permet toutefois de faire de la start-up une porte d'entrée sur les données d'un grand groupe avec lequel elle a conclu un partenariat.[81]

La qualité des d'informations échangées et du dialogue lors de la souscription d'un contrat de cyberassurance est donc perfectible sur tous les segments.

Souscrire une cyberassurance implique de réaliser un audit de souscription technique, contractuel et de gouvernance. Cela supposerait dans certaines hypothèses de se rendre sur site afin de comprendre comment est appréhendé le risque cyber par l'assuré et quelle est son activité.[82] Cette visite sur site n'est pas impérative car l'important est d'aborder avec l'assuré en direction la cyberassurance et de pouvoir accéder à ses données techniques, contractuelles et organisationnelles. Il s'agit de comprendre les procédés techniques utilisés par l'assuré, clarifier le processus interne de décision quant à la cybersécurité, et cerner le panorama d'assurances en cours d'effet. Une visite de risque n'est pas envisageable ni nécessaire à chaque souscription cyber. Elle peut parfois ne rien apporter de plus puisque les données sont souvent hébergées dans des *data centers*.

Le plus adapté semblerait de réaliser une ou des réunions en physique ou par visioconférence avec l'assuré afin de cerner son exposition au risque cyber.[83] Cette réunion doit aussi prendre place à plusieurs car il est encore fréquent que la prise de conscience du

[81] Cette remarque fait écho à l'intérêt de sécuriser la chaîne de traitement de données par des contrats de cyberassurance et des contrats de sous-traitance et de partenariat cyber résilients.
[82] BLOUIN, Thibault, *L'assurance est-elle capable de protéger les entreprises contre la cybercriminalité ?*, Banque & Stratégie n°352, ENASS Papers 12, Novembre 2016.
[83] MARGUINAUD, Xavier, Cyber Underwriting Manager chez Tokio Marine HCC, Entretien téléphonique, Août 2017.

risque cyber se réalise dans la phase de souscription d'une cyberassurance.[84] Cela démontre d'ailleurs le potentiel que présente l'assureur à dynamiser la gestion de ce risque.

L'assureur cyber doit accompagner son client dans cette prise de conscience. Cet entretien est déjà l'occasion pour lui de mettre en application sa qualité de gestionnaire de risque en y introduisant des consultants afin que les meilleures décisions en cybersécurité et en cyber résilience soient prises. Autour de l'assureur et de ses partenaires (courtiers, experts) devront être présents la direction générale, la direction des services d'information, le responsable de la sécurité des systèmes d'information, le *risk manager* et la direction juridique, afin de cartographier les risques et d'évaluer leur probabilité d'occurrence ainsi que le coût induit. Cela permet, avant tout sinistre, de mettre en lumière les failles du système d'information.

Cette approche novatrice du risque cyber permet de cerner les besoins en cyberassurance de l'assuré et d'adapter le contrat cyber à son profil sans pour autant établir un contrat en sur-mesure. Le contrat cyber est un contrat à tiroirs, l'assureur peut créer de façon générique des garanties et choisir de n'en proposer que certaines d'entre elles au sein des volets dommages et de responsabilité civile.

Un phénomène de régionalisation des garanties se dessine. Des garanties sont créées et ne sont souscrites que dans certaines régions. Les manières de souscrire et d'envisager le risque cyber sont encore différentes à l'international. Ces garanties régionalisées sont adaptables aux diverses réglementations.[85]

Cette approche du risque doit persévérer en cours de vie du contrat. L'assureur cyber ne peut se contenter de laisser un contrat cyber suivre son cours et agir uniquement sur des demandes de modification de l'assuré. L'assuré n'a parfois pas conscience que le progrès technologique au sein de sa structure et les éventuelles modifications de procédures et d'infrastructures peuvent avoir un impact sur son contrat d'assurance. C'est à l'assureur de prendre la main sur l'évolution du contrat par rapport à la situation de l'assuré et de le mettre à jour par des contrôles réguliers, avec pour strict minima le temps du renouvellement tacite du contrat. Le risque cyber nécessite d'être maîtrisé au-delà du cadre d'un sinistre.

[84] PIRSON, Astrid-Marie, Directrice de la souscription Hiscox France, Atelier cybersécurité, Paris, Juin 2017.
[85] MARGUINAUD, Xavier, Cyber Underwriting Manager chez Tokio Marine HCC, Entretien téléphonique, Août 2017.

L'assureur cyber doit se tenir à proximité de son assuré, et le courtier a un rôle à jouer dans cette approche novatrice du risque.

ii. La confidentialité des échanges entre assureur, prospect et assuré

Les négociations d'un contrat de cyberassurance, à ce qu'elles impliquent beaucoup de personnes et d'informations, peuvent durer plus d'une année, alors même que la souscription du contrat n'est pas certaine. Dans ce contexte, les prospects demeurent réticents à communiquer à l'assureur et ses partenariats les nombreuses informations confidentielles nécessitées, tout en devant pointer les défaillances techniques et organisationnelles de leurs structures. Cette observation est aussi valable pour les particuliers qui souscrivent un contrat de cyberassurance. Il s'agit ici d'introduire leur vie privée. L'assureur cyber doit mettre en place une politique de confidentialité dans le dialogue de souscription tout en la poursuivant en cours de vie du contrat si ce dernier est conclu. La confidentialité en cours de vie du contrat peut être gouvernée par des clauses contenues dans le contrat d'assurance. La question semble de prime abord plus délicate en période précontractuelle. Certains proposent la mise en place d'une plateforme neutre et sécurisée de communication et d'échange d'informations entre les assurés et les assureurs. Cela permet de standardiser les processus de confidentialité et d'utiliser globalement les données fournies. Trois manières de développer cette plateforme sont proposées en ce qui concerne les lignes d'assurance professionnelles : une extension de la plateforme d'assistance aux victimes de cyber malveillance mise en place par l'Agence nationale de la sécurité des systèmes d'information et le Ministère de l'Intérieur, une plateforme chez un tiers de confiance sans visée commerciale, un observatoire national du risque cyber, sur le modèle de l'Observatoire National des Risques Naturels. Cette dernière structure, selon les auteurs, permettrait par un processus d'anonymisation, la mise en place de statistiques fiables qui fonderaient de meilleures quantification et tarification du risque.[86] L'idée de la plateforme d'échange et de communication est intéressante. Cela dit, des réserves doivent être émises à impliquer le secteur public dans la gestion du risque cyber dès la période précontractuelle de souscription d'un contrat de cyberassurance, à ce qu'aucun filet de sécurité public de réassurance n'existe pour l'heure, ni même grande implication des Etats dans la sensibilisation aux bonnes pratiques de cyber résilience. L'idée d'un partenariat entre

[86] SYSTEM X, Institut de recherche technologique, *La maîtrise du risque cyber sur l'ensemble de la chaîne de sa valeur et son transfert vers l'assurance, Résultats du séminaire de recherche*, Maîtrise du risque cyber et assurance, Novembre 2015 - Juillet 2016, 14 p.

l'Agence nationale de la sécurité des systèmes d'information et les assureurs privés semble plus adaptée. En tout hypothèse, les échanges précontractuels peuvent donner lieu à la conclusion d'un accord de confidentialité entre l'assureur, ses partenaires et l'assuré.

De même, la notion de confidentialité, comme nous l'avions évoqué, peut rester conflictuelle en cours de vie du contrat et notamment lors de la survenance d'un sinistre, car l'assuré aura dévoilé de nombreuses informations à l'assureur en phase de souscription qui ne seront pas traitées par le même service au sinistre. Impliquer une tierce entité neutre et experte dans les échanges de souscription mais aussi dans les échanges de gestion de sinistre, sur une même plateforme, paraît une idée intéressante et à développer.

b) Spécialiser les offres de cyberassurance selon les secteurs d'activité

Si les programmes de cyberassurance présentent des garanties adaptées au risque cyber, ils gagneraient à se spécialiser par secteur d'activité car ces derniers ne présentent pas la même exposition au risque cyber. Ils ne sont en effet pas susceptibles de subir les mêmes typologies d'attaque ni les mêmes types de dommages. Le risque cyber peut être ciblé, de masse, d'intensité, de fréquence, et les diverses combinaisons qui en ressortent, tout comme il est plus probable qu'il cause des dommages matériels ou immatériels selon le secteur d'activité de la cible. Les modules de couverture actuels restent généraux. Par exemple, l'obligation de notifier concerne tout responsable de traitement, et cette notion s'applique à une multitude d'acteurs depuis 1978. Il pourrait être envisagé d'ajouter un volet de garanties spécifiques aux différents secteurs d'activité.

Le risque cyber est difficile à qualifier et à quantifier. Sur le marché français, qui est encore jeune, mais aussi à l'international, les assureurs peinent à modéliser et qualifier les risques cyber par secteur d'activité, ce qui participe de l'illisibilité des offres de cyberassurance[87] et de leur tarification perfectible. Les contrats de cyberassurance apporteraient une réponse plus experte au risque cyber s'ils étaient spécialisés par secteurs d'activité.

Par exemple, les banques et les services financiers sont pleinement conscients de leur attractivité quant au vol de données et sont leaders dans l'implémentation de systèmes de

[87] TELECOM ParisTech, Alumni, *Livre blanc : comment « débloquer » le marché de l'assurance cyber en France ?*, Juin 2017, 11 p.

cybersécurité ainsi que dans la mise en place de mesures de prévention contre le vol de données. La Bank of America a dépensé plus de 400 millions de dollars dans la cybersécurité en 2015 et le *Chief Executive Officer* a annoncé en janvier 2016 que le budget affecté à la cybersécurité n'était pas limité. JP Morgan Chase and Co. a annoncé une augmentation au double de son budget cybersécurité de 250 millions en 2015 à 500 millions en 2016.[88]

Une analyse des attaques cyber dans les différents secteurs d'activité démontre qu'il y a eu une augmentation du taux de fuite de données dans les secteurs de la vente, des technologies de l'information, des services et de la manufacture. Les fuites de données ont été considérablement réduites dans le secteur des services financiers, alors que ce secteur est particulièrement visé afin d'accéder à des données personnelles dont bancaires. Cela confirme que des investissements en sécurité et en protection de données ont été réalisés dans ce secteur. La même baisse de taux est constatable dans le secteur des services de santé en ce qui concerne les violations de données, bien que cela soit contrebalancé par une augmentation importante des cyber extorsions. Des attaques récentes ont de manière répétée ciblé des sites sociaux tels que Fling, Matel, ou Ashley Madison, afin de pouvoir procéder plus aisément à du chantage et de l'extorsion.[89]

La cyberassurance devrait alors prendre en considération cette diversité de risques cyber pour adapter les garanties et prestations de gestion de crise et *in fine* de risque aux différents secteurs d'activité. Une réponse plus adaptée permettrait bien sûr de répondre plus précisément aux besoins des assurés, aussi d'augmenter le volume de souscriptions, de gérer plus facilement les sinistres et de maturer le marché de la cyberassurance.

Willis Towers Watson propose par exemple un nouveau produit cyber adapté au secteur de l'aviation, CyFly. Ce produit a été développé avec AIG. Il contient une extension des pertes d'exploitation à des tiers car les entreprises du secteur de l'aviation dépendent de services de nombreux tiers pour assurer une continuité d'activité. Les frais de maintenance des avions ou les frais de sécurité de l'aéroport sont couverts.[90]

---

[88] CENTRE FOR RISK STUDIES, University of Cambridge Judge Business School & Risk Management Solutions (RMS), *2017 Cyber Risk Landscape*, 18 p.
[89] CENTRE FOR RISK STUDIES, University of Cambridge Judge Business School & Risk Management Solutions (RMS), *2017 Cyber Risk Landscape*, 14 p.
[90] WILLIS TOWERS WATSON, *Willis Towers Watson launches innovative new cyber product for global airlines*, Press Release, Avril 2017.

Cette exigence d'adaptation des programmes de cyberassurance nécessite de modéliser le risque cyber selon les différents secteurs d'activité. Des méthodes de modélisation ont été développées mais demeurent perfectibles, notamment sur la quantification de l'exposition silencieuse au risque cyber.

c) Développer les offres de cyberassurance au-delà de la sphère professionnelle

Le cyber risque concerne chaque individu mais les assurés et prospects sont plus ou moins conscients, plus ou moins impliqués dans le processus de cyber résilience. Les polices de cyberassurance nécessitent d'être développées par secteur d'activité mais aussi au-delà de la sphère professionnelle. Il est aujourd'hui difficile de concevoir l'idée selon laquelle le risque cyber qui menace les entreprises restera à leurs portes, à ce que ce risque ne connaît pas de frontière. La sphère privée et la sphère professionnelle peuvent être la faille de l'une de l'autre lors de la survenance d'une cyberattaque. Les frontières des sphères professionnelles et privées s'amenuisent à ce que l'interconnectivité et l'influence des nouvelles technologies sur le monde du travail, et les mutations qu'elles entraînent, tel que *Bring Your Own Device* ou le télétravail, se développent.

Les objets connectés représentent là encore un enjeu puisqu'ils envahiront le quotidien professionnel et privé de chaque individu, et pourront servir ces deux finalités.

Des assureurs proposent des offres spécifiques de cyberassurance pour les particuliers. AIG, le premier assureur cyber sur les lignes professionnelles, a mis en vente cette année le produit Family CyberEdge au profit de sa clientèle privée. Ce produit prend en charge la cyber extorsion et le cyber harcèlement, ainsi que les frais de restauration de données, de gestion de crise et de réputation. Nous constatons que les garanties sont adaptées au risque cyber susceptible de porter atteinte aux individus dans leur vie privée.

Nous développons tout au long de notre raisonnement la logique selon laquelle l'assureur cyber doit participer de la gestion de risque en sortant de son rôle traditionnel. Dans le contexte précédemment développé, AIG collabore avec K2 Intelligence, une entreprise de services de cyberdéfense, en vue de prodiguer à ses assurés des informations qui leur permettront de manager leur risque cyber de façon proactive. K2 Intelligence est en partie détenu par AIG. Créer des polices de cyberassurance en partenariat avec des entreprises de

cybersécurité s'inscrit dans le processus de cyber résilience. Le public des particuliers est particulièrement novice en matière de cybersécurité. Ce partenariat permet aux clients de bénéficier d'outils, de réseaux sécurisés avec des comptes de gestion des informations personnelles traitées dans les activités privées, des services de formation à la cybersécurité pour tous les membres de la famille, et une mise à disposition d'experts en fraude.[91] D'autres experts comme des experts en communication pourraient être associés à la création du produit et impliqués dans la vie du contrat.

AIG n'est pas le seul assureur à se positionner sur le marché. Chubb a ajouté une garantie de cyber harcèlement dans son produit U.S. Masterpiece Family Protection, comme cet assureur avait commencé à le faire depuis 2015 au Royaume-Uni. Hartford Steam Boiler Inspection and insurance Co. (HSB), qui fait partie du groupe Munich Re, a commercialisé le produit HSB Home Cyber Protection. Cette garantie est intégrée dans les polices d'assurance de propriétaires et locataires des compagnies d'assurances partenaires de HSB.[92] Cette extension est intéressante au regard de l'avènement des objets connectés, car l'habitation sera une *smart home*. Les cyberattaques sur des systèmes d'information opérationnels pourraient concerner des habitations privées, et causer des dommages immatériels, matériels et corporels.

Le risque cyber est un risque omniprésent. Il est maximisé par son fort potentiel catastrophique et vient questionner les assureurs sur leur capacité de prise en charge financière, particulièrement au niveau de la réassurance.

2 Développer la capacité de la cyberassurance

Améliorer la capacité de la cyberassurance sur le risque cyber suppose principalement de manager l'accumulation de risque afin de pouvoir tarifier plus justement et d'y risquer plus de capacité. Il est aussi possible d'actionner les mécanismes de la réassurance et des marchés financiers, tout autant qu'impliquer les Etats dans le financement des risques catastrophiques envers lesquels ils ont une part de responsabilité.

[91] La combinaison d'assurances cyber et fraude pour les particuliers est un point à réfléchir.
[92] INSURANCE JOURNAL, *AIG latest to bring cyber insurance to personal lines high-net-worth clients*, April 2017.

a) Manager l'accumulation de risque cyber

Les impacts du risque cyber sont d'une telle complexité et dépendent d'un tel nombre de variables que le marché de l'assurance est transfiguré par ce risque dans sa globalité.

Pour l'heure, dans l'ensemble, le risque cyber est explicitement et implicitement couvert par plusieurs lignes d'assurance, sur ses conséquences matérielles et immatérielles, ce qui rend le marché de la cyberassurance illisible et nuit à sa segmentation. En effet, la capacité globale d'un assureur sur ce risque, au-delà des lignes spécifiques et des extensions cyber constituant des prises en charge affirmées, peut être challengée par l'exposition silencieuse au risque cyber dans les polices traditionnelles.

La capacité de l'assureur reste pour autant challengée par son exposition affirmée au risque cyber, puisqu'ajouter des garanties cyber dans plusieurs lignes de façon affirmée en ne bénéficiant que de données historiques limitées dans des conditions de marché difficiles ne permet pas d'aboutir à une tarification adéquate.[93]

Un cyber assureur voit donc sa capacité challengée sur le risque cyber par un assuré qui a souscrit plusieurs contrats auprès de sa compagnie, ou par un assuré ayant subi un sinistre pouvant être couvert par plusieurs contrats d'assurance.[94]

La capacité de l'assureur peut aussi être challengée au sein de son portefeuille cyber par la problématique de l'accumulation de risque. Le risque cyber est potentiellement sériel et systémique, notamment du fait de l'interconnectivité des technologies utilisées par les assurés. De plus en plus d'attaques cyber impactent de multiples entreprises en un simple évènement. Le risque cyber est donc un éventuel risque de masse, plus probablement lorsque son origine est malveillante, et peut sinistrer une large partie d'un portefeuille cyber. La capacité du cyber assureur est donc aussi challengée lorsque plusieurs assurés du portefeuille sont sinistrés par le même évènement ou que ces assurés utilisent les mêmes technologies de l'information. Ces assurés peuvent par exemple héberger leurs données ou système d'information chez le même hébergeur.[95] Un assureur cyber peut par exemple avoir au sein de son portefeuille cyber de

[93] CENTRE FOR RISK STUDIES, University of Cambridge Judge Business School & Risk Management Solutions (RMS), *2017 Cyber Risk Landscape*, 39 p.
[94] ZICRY, Laure, Cyber Risks Practice Leader chez Gras Savoye, *Table ronde # 1 Cyber assurance*, Cercle des Femmes dans la Cybersécurité, Juin 2017.
[95] ZICRY, Laure, *supra*.

nombreuses institutions financières. Ces institutions financières vont utiliser plus ou moins les mêmes techniques de cybersécurité et qui en toute hypothèse sont propices à l'interconnexion. Si une cyberattaque vise cette technologie, alors ce n'est pas un assuré qui est impacté mais une partie du portefeuille.[96] Ce même scénario peut être réitéré dans chaque secteur d'activité, au sein duquel il est fort probable de constater des similitudes de cybersécurité.

La nouvelle technologie des objets connectés ne fait pas défaut à cette observation. Un objet connecté comme une montre est facilement accessible à une tierce personne non autorisée et constitue une porte ouverte sur le réseau Internet. Il existe actuellement 28 millions d'objets connectés, 50 millions selon les prévisions pour 2020. Ces objets connectés, qui incorporent tous les domaines du quotidien (le transport, les soins médicaux, l'infrastructure des bâtiments, les processus industriels...) sont vulnérables à des manipulations malicieuses. Ces systèmes ont été pensés sans grande attention portée à la cybersécurité et ont pour l'heure de faibles niveaux de protection contre le piratage. Les assureurs vont devoir prendre en considération ce potentiel de vulnérabilité dans leur analyse de risque ainsi que le rôle de ces objets dans les attaques cyber causant des dommages matériels.[97]

Cela fait écho à de précédentes réflexions. L'assureur a intérêt à spécialiser ses lignes cyber par secteur d'activité afin de mieux appréhender ce risque d'accumulation. L'assureur a intérêt à se positionner sur de la gestion de risque afin d'influencer des partenaires techniques à développer des technologies différentes et plus ou moins interconnectables[98] mais aussi d'influencer ses assurés dans leurs choix de cybersécurité. En effet, ces divers exemples illustrent encore le fort potentiel de l'assureur à porter les bonnes pratiques de cybersécurité.

De même, les diverses institutions de régulation financière, à l'instar de la Prudential Regulatory Authority au Royaume-Uni qui en est la plus active sur le sujet cyber, incitent les assureurs à identifier, quantifier et manager leur exposition au risque cyber, que cette dernière soit affirmée ou silencieuse. En effet, le risque cyber peut être un facteur d'insolvabilité. Du fait de cette exposition silencieuse au risque, les assureurs ne réalisent peut-être pas l'étendue de leur exposition globale et n'ont peut-être pas impacté l'envergure de leur exposition sur la

[96] MARGUINAUD, Xavier, Cyber Underwriting Manager chez Tokio Marine HCC, Entretien téléphonique, Août 2017.
[97] CENTRE FOR RISK STUDIES, University of Cambridge Judge Business School & Risk Management Solutions (RMS), *2017 Cyber Risk Landscape*, p 28.
[98] Ce qui peut aussi relever des pouvoirs publics.

somme des primes collectées. Les assureurs doivent revoir leurs lignes afin d'identifier les ambigüités de couverture et le coût du risque que cela représente. Les lignes impactées par le risque cyber sont potentiellement celles consacrées aux risques maritimes, d'aviation, d'énergie, de responsabilité civile et de dommages. La tendance chez les assureurs anglo-saxons est d'inclure dans les polices traditionnelles des exclusions du risque cyber.

Gérer cette accumulation de risque au sein d'un portefeuille cyber et sur le portefeuille global est un des challenges clés auxquels s'expose l'assureur en vue de développer un portefeuille cyber résilient.

Dans l'attente d'une réglementation européenne qui viendra certainement, imposant un pourcentage de réserve en fonction du volume de souscription, une des premières solutions qui s'offre aux assureurs est de diversifier leur portefeuille cyber. Cela peut se faire au regard de trois critères : la localisation géographique, le secteur d'activité, le segment de cible.[99] Il est moins probable qu'un assuré éloigné d'un autre selon ces trois critères soit impacté par la cause du sinistre cyber de cet autre assuré.

Les assureurs les plus matures du marché de la cyberassurance ont développé ces dernières années des scénarii de simulation de crises afin d'estimer leur maximum de perte face des catastrophes cyber. Ces scénarii varient dans leur approche du risque cyber, du plus simpliste au plus complexe des systèmes avec des éventuels apports externes d'expertise et d'analyse de risque. Ils permettent une réflexion en amont sur des sinistres catastrophes. Sous la pression des organismes de régulation du marché de l'assurance et à ce que des solutions commerciales de modélisation se développent, de plus en plus de compagnies d'assurance, y compris nouvelles entrantes sur le marché de la cyberassurance, sont capables d'adopter une vision plus cohérente de ce risque et d'organiser une meilleure répartition de leur capital sur le marché en établissant leur appétit sur le risque cyber.[100] Des standards communs d'analyse de risque existent pour permettre aux assurés d'identifier, de quantifier et de rapporter leur cyber exposition aux assureurs de façon harmonisée.[101]

[99] MARGUINAUD, Xavier, Cyber Underwriting Manager chez Tokio Marine HCC, Entretien téléphonique, Août 2017.
[100] CENTRE FOR RISK STUDIES, University of Cambridge Judge Business School & Risk Management Solutions (RMS), *2017 Cyber Risk Landscape*, 39 p.
[101] VIVAR, Mariona, *Réassurance : Et si le risque cyber bénéficiait d'un 'filet de sécurité' de l'Etat ?*, News assurances pro, Mars 2017.

Le système est cependant perfectible et la prochaine étape serait d'arriver à modéliser l'exposition silencieuse au risque cyber des polices traditionnelles. A l'heure actuelle, le mécanisme d'agrégation technique se limite aux polices dont l'exposition au risque cyber est affirmée. Cela concerne par exemple les lignes spécifiques cyber mais aussi les polices fraude ou les polices de responsabilité civile qui contiennent des extensions cyber. Personne n'est encore en mesure de monitorer les polices qui n'excluent pas le risque cyber sans pour autant explicitement le couvrir. Une police couvrant la responsabilité des dirigeants qui n'exclut pas le risque cyber prend pour l'instant en couverture ses conséquences dans les postes qu'elle a prévus, telle que la chute du cours de bourse par exemple. Il serait alors nécessaire de traquer les exclusions de risque et de prendre en compte toutes les autres polices dans les scénarii catastrophes. Cela est loin d'être simple car les assureurs utilisent des outils informatiques qui sont des survivances de tel ou tel service ou branche. Le Lloyds a conseillé aux assureurs de considérer comme exposée au risque cyber la somme de toutes les polices souscrites, mais cela n'aboutit pas une juste vision de l'impact du risque cyber. Il paraît plus judicieux de considérer l'exposition affirmée au risque comme l'exposition minimum et d'affiner les outils de modélisation de risque sur l'exposition silencieuse. Personne n'a encore la clé pour gérer l'accumulation de risque cyber, nous sommes au début de ce processus.[102]

In fine, souscrire un contrat de cyberassurance devrait présenter l'avantage de créer une capacité spécifique sur le risque cyber et de protéger par là même, en théorie, la capacité des autres assurances de l'assuré.

b) Financer les risques catastrophiques

Le financement des risques catastrophiques amène lui aussi à l'innovation dans le secteur de la réassurance et des marchés financiers. Le financement privé du risque cyber trouve toutefois ses limites là où la responsabilité des Etats devrait commencer.

i. Le rôle limité de la réassurance privée

L'assureur qui a diversifié son portefeuille et qui reste prudent peut sur les risques les plus complexes faire appel à la réassurance. Les réassureurs participent activement à l'augmentation de capacité en première ligne. De par leur exposition exacerbée au risque

[102] VEZIO, Philippe, Managing Director chez Tokio Marine HCC, entretien téléphonique, Août 2017.

cyber, les réassureurs ont rapidement développé une dynamique d'agrégation. Le marché de la réassurance continuera de progresser en fonction de la croissance du marché de la cyberassurance en première ligne. Cela se fera au moyen de cessions de risque et des formes additionnelles de réassurance qui deviendront pratique courante à mesure de l'amélioration des techniques de quantification du risque.[103]

Il reste cependant difficile d'évaluer l'impact potentiel d'un sinistre systémique et de mettre au point des scénarii catastrophes. Les réassurances introduisent donc des limites annuelles de couverture dans les traités de réassurance et ce y compris sur des structures en quotepart. Les définitions du risque cyber dans les traités de réassurance n'ont pas encore été confrontées à des sinistres de grande ampleur. Cela est source d'insécurité pour un assureur qui choisirait de se couvrir en réassurance par un traité en excédent de sinistre par événement.[104] Les réassureurs sont plus exposés au risque d'insolvabilité consécutif à l'accumulation de risque cyber et à son management perfectible. Certains réassureurs tels que Swiss Re ou Munich Re présentent une activité de réassurance et d'assurance en première ligne en relation avec des clients. Cela multiplie leur exposition au risque cyber sur plusieurs niveaux d'assurance. La plupart des réassureurs ont décidé de recentraliser la réassurance afin d'assurer un meilleur contrôle des prises de risque.[105]

Les réassureurs établissent des partenariats avec des entreprises du secteur de la cybersécurité et du secteur de l'analyse de risque afin de combler le vide d'information historique et de proposer des offres plus adaptées. Les réassureurs ont développé une analyse plus experte du risque du fait de leur forte exposition. Cela dit, ils se heurtent à la même limite d'absence de connaissance pratique. Les conséquences d'un risque complexe sont découvertes à sa réalisation. Les réassureurs participent activement au développement des modèles d'agrégation.

Afin de développer la capacité cyber, il est aussi envisageable de créer des véhicules d'investissement destinés à faire supporter une partie du risque à des investisseurs sur les marchés financiers. Des initiatives de création de titres assurantiels en couverture de risque

[103] CENTRE FOR RISK STUDIES, University of Cambridge Judge Business School & Risk Management Solutions (RMS), *2017 Cyber Risk Landscape*, 37 p.
[104] ASSOCIATION DES PROFESSIONNELS DE LA REASSURANCE EN FRANCE, *Etude sur les « cyber risques » et leur (ré)assurance*, Juin 2016, 21 p.
[105] VEZIO, Philippe, Managing Director chez Tokio Marine HCC, entretien téléphonique, Août 2017.

cyber ont été constatées.[106] Dans sa dernière étude Sigma sur le risque cyber, Swiss Re indique que le marché des titres assurantiels pour le risque cyber est encore naissant mais qu'il pourrait se développer.[107] Selon Benjamin Jacquet, ILS Underwriter & Cyber Risk Expert chez Crédit Suisse Insurance Linked Strategies, l'accumulation de l'exposition des assureurs au risque cyber et la capacité à tarifier et à modeler ce risque sont les deux challenges que l'essor de ce marché doit affronter, tout en confirmant que le risque cyber représente une opportunité pour les marchés financiers. Le récent *ransomware* WannyCry a mis en lumière le potentiel extrême de perte financière que pouvait représenter une cyberattaque, soulignant le besoin non seulement de réassurance mais aussi d'une profonde réserve de capital ILS, ou d'un espace de réassurance alternative.[108]

Pour l'heure, la capacité de financement des assureurs reste limitée et certains acteurs du marché appellent à l'implication des pouvoirs publics sur cette problématique.

ii. L'implication et la responsabilisation des Etats

Dans un scénario catastrophe, ce serait-il pas pertinent de requérir le soutien financier des pouvoirs publics ? Le risque cyber est un risque global, à ce qu'à terme tout élément, objet ou personne, sera connecté et interconnecté, et ce à une échelle mondiale. Le sinistre cyber catastrophique aurait des conséquences désastreuses pour la vie économique d'un pays.

Il est aussi possible d'envisager un financement public de la cyberassurance lorsque l'on constate que des services publics, de première nécessité, ou d'importance vitale pour les Etats, peuvent être tout autant impactés par des cyberattaques que le secteur privé. C'est le cas des hôpitaux qui sont visés de manière répétée par des attaques de cyber extorsion ou des sites industriels stratégiques.

Dans ce contexte, les pouvoirs publics pourraient intervenir financièrement de plusieurs manières. Il est possible d'imaginer un système de réassurance dont les pouvoirs publics seraient le dernier échelon. Le risque cyber catastrophique peut être transféré en première ligne à l'assureur, et selon l'éligibilité du risque, à un deuxième niveau qui serait de

[106] Les Insurance-linked securities (ILS) sont des instruments financiers dont la valeur est guidée par des sinistres assurantiels. Ce mécanisme de financement s'applique aussi aux dommages matériels causés par des catastrophes naturelles.
[107] SWISS RE INSTITUTE, Sigma, *Cyber : getting to grips with a complex risk*, No 1/2017, 2017, 34 p.
[108] EVANS, Steve, *Regulation and analytics can help cyber ILS market flourish*, Seeking Alpha, Juin 2017.

la réassurance privée et pour les risques cyber les plus conséquents, à un troisième niveau de réassurance publique. Il serait même possible d'ajouter un échelon de dernier recours de réassurance publique internationale. Swiss Re estime qu'un filet de sécurité public pourrait trouver sa pertinence face au risque cyber le plus complexe, voire, inassurable. Sont visés des sinistres tels que la perturbation généralisée d'infrastructures ou de réseaux d'une certaine importance, pouvant engendrer des cumuls de dommages.[109]

Il est aussi envisageable de créer un organisme public de réassurance, ou une sorte de garantie de l'Etat, bien que ce mécanisme soit remis en question par les libertés européennes et le droit de la concurrence, mais pourrait devenir international.

Certains auteurs ont avancé que le financement du mécanisme de réassurance publique pourrait provenir des sanctions infligées par les différentes autorités compétentes, ou d'une taxe sur les contrats cyber ou encore sur les produits ou services liées aux technologies de l'information.[110] L'idée du financement par le montant des sanctions administratives est intéressante dans l'hypothèse où ces dernières ne seraient pas assurables. A défaut, le mécanisme reviendrait à ce que des assureurs privés financent la réassurance publique.

Dans la continuité de ce raisonnement, nous pouvons renverser le point de vue et s'intéresser à l'implication des Etats dans la cyber activité. L'activité cyber des Etats est traditionnellement cantonnée aux domaines exécutifs et ne provoque pas de dommages au-delà du plan politique, militaire, et diplomatique. De récentes attaques suspectées d'être sponsorisées par les Etats ont toutefois causé des pertes dans le secteur civil et privé. Par exemple, la cyberattaque subie par l'entreprise Sony en 2014 serait selon les Etats-Unis d'Amérique de source nord-coréenne. Il existe de même des allégations selon lesquelles la Corée du Nord serait impliquée dans la soustraction par cyberattaque de millions de dollars d'une douzaine de banques.[111]

Cette implication effective des Etats dans la cyber activité produit bien des impacts sur le marché de la cyberassurance. Par exemple, en 2016 le groupe de hackers ShadowBrokers a rendu disponible un fichier contenant un panel d'armes de cyber hacking obtenu de l'Equation

[109] SWISS RE INSTITUTE, Sigma, *Cyber : getting to grips with a complex risk*, No 1/2017, 2017, 33 p.
[110] TELECOM ParisTech, Alumni, *Livre blanc : comment « débloquer » le marché de l'assurance cyber en France ?*, Juin 2017, 19 p.
[111] CENTRE FOR RISK STUDIES, University of Cambridge Judge Business School & Risk Management Solutions (RMS), *2017 Cyber Risk Landscape*, 8 p.

Group, une des équipes de cyber hacking de la National Security Agency des Etats-Unis d'Amérique. Ces outils extrêmement qualitatifs permettaient de pénétrer des firewalls standards tels que Cisco SAS, Fortinet FortiGate et Juniper SRX. Des hackers peu scrupuleux avaient donc la possibilité en usant de ces outils d'accéder aux systèmes d'information des entreprises qui utilisaient ces firewalls. En urgence, les semaines suivant la diffusion publique du dossier, des patches de sécurité ont été élaborés et des mesures de prévention ont été établies. Nous constatons toutefois bien dans cette espèce que l'implication des pouvoirs publics dans la cybersécurité peut avoir des conséquences sur un portefeuille d'assurés, et ce même de manière systémique.[112]

Cette implication des Etats dans une sorte de cyber guerre soulève le débat de l'assurabilité privée des conséquences d'une sinistre cyber causé à des entreprises du secteur privé ou des particuliers par une action d'origine publique. L'attribution d'une attaque cyber est très difficile. Différencier l'attaque criminelle de l'attaque sponsorisée par un Etat serait un challenge pour les assureurs. L'appétit des assureurs sur le risque cyber peut varier selon la proportion qu'en prend la cybercriminalité sponsorisée par les Etats, potentiellement conséquente. Il s'agit là d'une menace majeure de risque systémique, les équipes cyber sponsorisées bénéficiant des ressources les plus performantes.

Dans la continuité, nous pouvons noter que les groupes terroristes ne sont pas encore en possession d'une capacité de cyber destruction, bien que certains groupes soient connus pour faire des recherches en ce sens.[113] Le problème d'attribution global des cyberattaques concerne aussi les actes de cyber terrorisme. Le cyber terrorisme fait débat lorsqu'il s'agit d'aborder le sujet des pools d'assurance. L'assurance couvrant les actes terroristes est globalement traitée à travers le monde de façon spécifique. Un filet de sécurité public existe pour ces risques. Aux Etats-Unis, les assureurs sont sommés de fournir une offre de couverture, et cela est automatiquement inclus dans l'assurance accident des salariés.[114] Le parallèle pourrait être établi quant à la prise en charge du risque cyber, ce que Swiss Re a effectué dans son étude Sigma, d'ailleurs. Le U.S. Terrorism Risk Insurance Program Reauthorization Act de 2015 ne couvre pas explicitement le risque cyber. Certains assureurs

[112] CENTRE FOR RISK STUDIES, University of Cambridge Judge Business School & Risk Management Solutions (RMS), *2017 Cyber Risk Landscape*, 9 p.
[113] The United Cyber Caliphate arm of Islamic State, par exemple.
[114] CENTRE FOR RISK STUDIES, University of Cambridge Judge Business School & Risk Management Solutions (RMS), *2017 Cyber Risk Landscape*, 10 p.

suggèrent donc que ce dernier s'applique en cas de cyberattaque ayant causé des dommages à des infrastructures stratégiques.[115] La question du filet de sécurité public est donc toujours en débat à l'heure actuelle. L'assurance n'apparaît pas comme l'instrument le plus adapté pour répondre à cette typologie de risque cyber, sur laquelle les divers gouvernements devraient s'impliquer.

[115] CRO FORUM, *Cyber resilience, The cyber risk challenge and the role of insurance*, Décembre 2014, 39 p.

Conclusion

Les programmes de cyberassurance forment une réponse adaptée au risque cyber parce qu'ils couvrent les dommages subis par l'assuré et les dommages subis par les tiers, tout en fournissant à l'assuré des prestations d'assistance et de gestion de crise. Les assurances traditionnelles n'apportent pas une telle réponse à ce risque parce qu'aucune d'entre elles n'est d'une nature mixte.

Toutefois, le cyber assureur doit persister dans l'innovation de son métier en transformant la gestion de crise en gestion de risque et en repensant la souscription de ce risque complexe. Les programmes de cyberassurance font partie d'un processus plus global de maîtrise de risque résiliente, qui ne dépend pas seulement de l'assureur, et qui implique des prises de décision managériales, techniques, comportementales, gouvernementales. L'assureur, par son point de vue panoramique sur les sinistres cyber et son rôle central dans la gestion de risque, peut contribuer à la cyber résilience en incitant l'assuré à améliorer sa gouvernance de risque et en dynamisant les relations avec les divers acteurs du processus. Un contrat de cyberassurance adapté est un contrat qui innove le modèle assurantiel en interface de gestion de risque.

Les programmes de cyberassurance, dans leur généralité, ne couvrent pas l'ensemble des conséquences d'une cyber atteinte puisque les dommages matériels n'en sont pas couverts. Une possibilité de cumul d'assurances en résulte à ce que les polices d'assurance traditionnelles sont de manière affirmée ou silencieuse exposées au risque cyber, et donc susceptibles d'en couvrir les dommages immatériels non exclus et les dommages matériels. Il est aussi possible d'aboutir à une absence de garantie des dommages matériels des sinistres cyber. Cette incertitude voire lacune de couverture nuit à la maturité du marché de la cyberassurance.

Plus en avant, l'absence d'exclusion du risque cyber dans de nombreuses polices traditionnelles amène à une dangereuse problématique d'accumulation de risque qui n'est, par son aspect silencieux, pas maîtrisée par les mécanismes de financement de l'assurance, et sous-tend une problématique de solvabilité des assureurs et plus encore des réassureurs. Le risque cyber est un risque protéiforme capable d'impacter le portefeuille cyber et le portefeuille global d'un assureur d'une capacité maximale encore inconnue et non maîtrisée.

Les mécanismes de modélisation et d'agrégation du risque doivent à l'avenir permettre un meilleur management de l'accumulation de ce risque. A ce que le marché de la cyberassurance prospéra, la capacité des assureurs et réassureurs se développera et s'affinera, au même titre que des mécanismes de réassurance publique apparaitront, lorsque l'engagement de la responsabilité des Etats sera questionné.

Le marché de la cyberassurance est toujours forte croissance. La majorité du marché se situe aux Etats-Unis et se concentre sur la violation de données à caractère personnel. Le volume de prime devrait atteindre 7,5 milliards de dollars en 2020 et peut-être 20 milliards de dollars en 2025.[116] Les assurés en cyberassurance recherchent aujourd'hui plus de garanties, augmentées en termes de montant et améliorées en termes de qualité. Les petites et moyennes entreprises souscriront des contrats de cyberassurance à ce que cette police sera de plus en plus demandée lors de passations de marché et que les sinistres cyber seront dévoilés et de plus fort impact. La cyberassurance n'est pas encore *mainstream* mais le devient, et concerne tous les secteurs d'activité. Les particuliers sont aussi un champ de prospection de la cyberassurance à fort potentiel. Le risque cyber finira par être assuré, même sans obligation d'assurance.

Aux assureurs de spécialiser les garanties, de globaliser la prise en charge du risque cyber, d'améliorer les bases de tarification, de répartir les capacités, de sécuriser les polices traditionnelles et d'améliorer la souscription et la gestion de ce risque évolutif en faisant de l'assurance la pierre angulaire du processus de cyber résilience.

[116] CENTRE FOR RISK STUDIES, University of Cambridge Judge Business School & Risk Management Solutions (RMS), *2017 Cyber Risk Landscape*, 36 p.

Bibliographie

ARTICLES

BICHARD, Jean Philippe, *Beazley : affaire Sony, une jurisprudence ?*, Cyber Risques NEWS, Juillet 2014.

BLOUIN, Thibault, *L'assurance est-elle capable de protéger les entreprises contre la cybercriminalité ?*, Banque & Stratégie n°352, ENASS Papers 12, Novembre 2016.

DESCAZEAUX, Martin, *Assurer son système d'information industriel contre une cyberattaque, c'est possible ?*, Le blog cyber-sécurité des consultants Wavestone, Wavestone Riskinsight, Décembre 2015.

EVANS, Steve, *Regulation and analytics can help cyber ILS market flourish*, Seeking Alpha, Juin 2017.

INSURANCE JOURNAL, *AIG latest to bring cyber insurance to personal lines high-net-worth clients*, April 2017.

LENIHAN, Rob, *Double trouble with 'silent silent' cyber*, Business Insurance, Juillet 2017.

SCHNEIDER, Laure, *Article Cyber-risques et cyber-assurances*, Banque & Stratégie n°336, ENASS Papers 9, Mai 2015.

VIVAR, Mariona, *Réassurance : Et si le risque cyber bénéficiait d'un 'filet de sécurité' de l'Etat ?*, News assurances pro, Mars 2017.

WILLIS TOWERS WATSON, *Willis Towers Watson launches innovative new cyber product for global airlines*, Press Release, Avril 2017.

CONDITIONS GENERALES D'ASSURANCE

AIG, Conditions générales Pack Cyber 072014.

BEAZLEY, Conditions générales Beazley Breach Response.

HISCOX, Conditions générales Data Risks.

TOKIO MARINE HCC, Conditions générales Cyber Security Insurance.

ETUDES

AIG, Expertise Sinistres, *Assurance cyber : analyse des principales tendances, Livre blanc sur la criminalité*, 2017.

ASSOCIATION DES PROFESSIONNELS DE LA REASSURANCE EN FRANCE, *Etude sur les « cyber risques » et leur (ré)assurance*, Juin 2016.

BENTZ, H., Thomas, *Is your cyber liability insurance any good ? A guide for banks to evaluate their cyber liability insurance coverage*, 2017.

CENTRE FOR RISK STUDIES, University of Cambridge Judge Business School, *Cyber insurance exposure data schema V1.0*, Cyber Accumulation Risk Management, Cambridge Risk Framework, 2015.

CENTRE FOR RISK STUDIES, University of Cambridge Judge Business School & Risk Management Solutions (RMS), *2017 Cyber Risk Landscape*.

CENTRE FOR RISK STUDIES, University of Cambridge Judge Business School, *The insurance implications of a cyber attack on the US power grid*, Business Blackout, Society & Security, Emerging Risk Report - 2015 Innovation Series.

CRO FORUM, *Cyber resilience, The cyber risk challenge and the role of insurance*, Décembre 2014.

LEYTON, *Libre blanc : les cyber risques*, Juin 2015.

SWISS RE INSTITUTE, Sigma, *Cyber : getting to grips with a complex risk*, No 1/2017, 2017.

SYSTEM X, Institut de recherche technologique, *La maîtrise du risque cyber sur l'ensemble de la chaîne de sa valeur et son transfert vers l'assurance, Résultats du séminaire de recherche*, Maîtrise du risque cyber et assurance, Novembre 2015 - Juillet 2016.

TELECOM ParisTech, Alumni, *Livre blanc : comment « débloquer » le marché de l'assurance cyber en France ?*, Juin 2017.

WORLD ECONOMIC FORUM, *The Global Risks Report 2016*, 11th edition, 2016.

LOIS ET REGLEMENTS

PARLEMENT EUROPEEN ET CONSEIL, Règlement (UE) 2016/679, 27 avril 2016.

PARLEMENT FRANÇAIS, Loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés, 6 janvier 1978.

MEMOIRES DE RECHERCHE

ALAU, Ingrid, *Les cyber-risques dans l'entreprise : enjeux et assurance*, Mémoire de recherche, Master 2 Droit des assurances, Institut des Assurances de Lyon, 2013.

FEREY Gaspard, GROROD Nicolas, LEGUIL Simon, *L'assurance des risques cyber, Comment tirer le meilleur parti de l'assurance dans un contexte de numérisation intensive ?*, Mémoire de fin de formation du Corps des mines, MINES ParisTech, TELECOM ParisTech, 2017.

SUPPORTS DE PRESENTATION DES ASSUREURS ET DES COURTIERS

AIG, *Autopsie d'un sinistre*, Risques de cybercriminalité, 30 juin 2017.

GRAS SAVOYE, Lignes financières, *Les cyber risques*, Association Nationale des Industries Alimentaires, avril 2015.

HISCOX, *Atelier cybersécurité*, Paris, Juin 2017.

HISCOX, *Protection des données personnelles, Comprendre le règlement européen*, 2017.

ZICRY, Laure, Cyber Risks Practice Leader chez Gras Savoye, *Table ronde # 1 Cyber assurance*, Cercle des Femmes dans la Cybersécurité, Juin 2017.

Lexique

Bring Your Own Device

Il s'agit de l'utilisation d'appareils informatiques personnels dans la sphère professionnelle. Cette utilisation pose des problèmes juridiques, de sécurité informatique et de gestion de risques.

Une variante de cette nouvelle pratique émerge dans certaines entreprises : Buy Your Own Device. C'est alors l'entreprise qui finance l'outil technologique que le salarié utilisera à des fins personnelles et des fins professionnelles.

Cloud computing

Il s'agit de la fourniture de ressources informatiques en service à la demande et par réseau. Dans le cadre de la gestion de son infrastructure informatique, une entreprise peut donc décider de disposer d'une capacité de stockage et de services informatiques externalisés.

Le *cloud* se divise en trois catégories de services : le SaaS soit le Software as a Service, le PaaS soit le Platform as a Service, l'IasS soit l'Infrastructure as a Service.

Le *cloud* peut être public (service accessible à plusieurs clients) ou privé (service pour un client), ou une combinaison des deux.

Cyber

Qui implique ou qui fait référence à l'utilisation des technologies de l'information.

Cyber assurance

Assurance spécifique visant à couvrir les conséquences des atteintes au système d'information et/ou aux données qu'il contient.

Cyberattaque

Intrusion non autorisée dans un système d'information avec ou sans transfert de données en provenance de ce système d'information, de manière manuelle par une personne avec un accès physique au système ou de manière automatisée par un programme informatique malicieux

Cyber criminalité

Selon l'Organisation des Nations Unies, la cybercriminalité consiste en tout comportement illégal faisant intervenir des opérateurs électroniques visant la sécurité des systèmes informatiques.[117]

La Commission européenne évoque une définition plus large : « tout infraction qui implique l'utilisation des technologies informatiques ».[118]

L'essor d'Internet et des nouvelles technologies a permis l'apparition d'infractions nouvelles mais a aussi facilité la commission des infractions dans leur globalité.

Nous retiendrons que la cybercriminalité concerne toute comportement illégal qui par l'intervention des technologies de l'information nuit intentionnellement à la sécurité des systèmes et des données.

Le terme de cybercriminalité a une coloration pénale et implique donc de viser des actes réprimés par la loi. Il est souvent utilisé en référence à tout acte cyber malveillant, sans forcément porter égard à sa répression légale qui de toute manière est borné par des frontières géographiques, au contraire de la cybercriminalité.

Cyber incident

Ce cyber incident est l'atteinte au système d'information et/ou aux données qui n'est pas intentionnelle.

Cyber résilience

La cyber résilience est la capacité à préparer et à s'adapter à des conditions changeantes, de résister et de récupérer rapidement suite aux perturbations subies du fait d'attaques ou d'incidents. La résilience est de la gestion de risque. La notion de cyber résilience est plus

[117] Cité par SCHNEIDER, Laure, *Article Cyber-risques et cyber-assurances*, Banque & Stratégie n°336, ENASS Papers 9, Mai 2015.
[118] Commission européenne, *Combattre la criminalité à l'ère numérique : établissement d'un Centre européen de lutte contre la cybercriminalité*, Communication de la commission au conseil et au parlement européen, 28 mars 2012.

transversale que la notion de cybersécurité, cantonnée au domaine technique d'information. La cyber résilience est une approche globale du risque cyber impliquant le facteur humain et les techniques d'informations dans une vision à court, moyen et long terme, préventive et corrective.

Le processus de cyber résilience au sein d'une structure est gouverné par quatre piliers : préparer, protéger, détecter et améliorer. La cyberassurance fait partie du quatrième pilier. Un assureur cyber résilient doit se positionne en tant que gestionnaire de risque et inciter l'assuré à mettre en place les meilleures pratiques de cybersécurité tout en lui permettant de comprendre les coûts d'un sinistre cyber par la qualification et la quantification des dommages. [119]

L'assureur a vocation à de positionner de façon décisive dans le processus de cyber résilience.

Cyber risque

Aléa qui implique les technologies de l'information et qui est susceptible de produire des dommages immatériels et matériels. Le cyber risque est complexe, protéiforme et d'une évolution constante. Il est donc possible d'utiliser la notion au pluriel ou au singulier de façon indifférente.

Cybersécurité

La cybersécurité consiste à réduire le risque d'atteinte à des infrastructures par des moyens physiques ou mesures de cyberdéfense contre des attaques et des incidents, dans le cadre de l'utilisation de systèmes d'information et de communication. La cybersécurité est de la réduction de risque et la résolution des atteintes techniques.

Darknet

Le darknet ou les darknets sont des réseaux qui ne sont pas reliés à l'Internet. Leur chemin d'accès n'est pas librement accessible et leur existence est fondée sur le principe de l'anonymat.

Il ne s'agit pas du *Deep Web*, qui regroupe des sites librement accessibles par Internet mais qui ne sont simplement pas indexés par des moteurs de recherche.

[119] CRO FORUM, *Cyber resilience, The cyber risk challenge and the role of insurance*, Décembre 2014, 6 p.

Donnée numérique

La donnée numérique est, selon le dictionnaire en ligne L'Internaute, la « représentation d'une information en vue d'un traitement automatique ».

Donnée à caractère personnel

Les données à caractère personnel sont toute informatique relative à une personne physique identifiée ou identifiable directement ou indirectement.

Pénalités PCI-DSS

PCI-DSS est l'acronyme anglophone de *Payment Card Industry DataSecurity Standard*. Il s'agit donc de l'acronyme du standard de sécurité des données de l'industrie des cartes de paiement qui s'applique à toute entité qui traite des données de cartes bancaires. Il ne s'agit pas d'une obligation légale mais contractuellement généralisée par les principaux acteurs du marché, Visa et MasterCard. Une entité non conforme à PCI-DSS s'expose à des pénalités financières.

Responsable de traitement de données

Personne physique ou morale qui détermine les finalités et les moyens du traitement de données. Cette personne est assujettie à une obligation de sécurité, de transparence, et de durée de conservation par le droit français et européen. Ces obligations sont sanctionnées pénalement, civilement et administrativement.

Système d'information

Un ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) qui permet de regrouper, de classifier, de traiter et de diffuser de l'information sur un environnement donné. Un système d'information est virtuel.[120]

Traitement de données

Toute opération portant sur des données numériques. A titre d'exemples, il peut s'agir d'enregistrement, de collecte, d'organisation, de conservation, d'adaptation, de modification,

[120] ALAU, Ingrid, *Mémoire de recherche, Les cyber-risques dans l'entreprise : enjeux et assurance*, Master 2 Droit des assurances, Institut des Assurances de Lyon, 2013.

d’extraction, d’utilisation, de consultation, de communication, de verrouillage, d’effacement, de destruction.

Table des matières