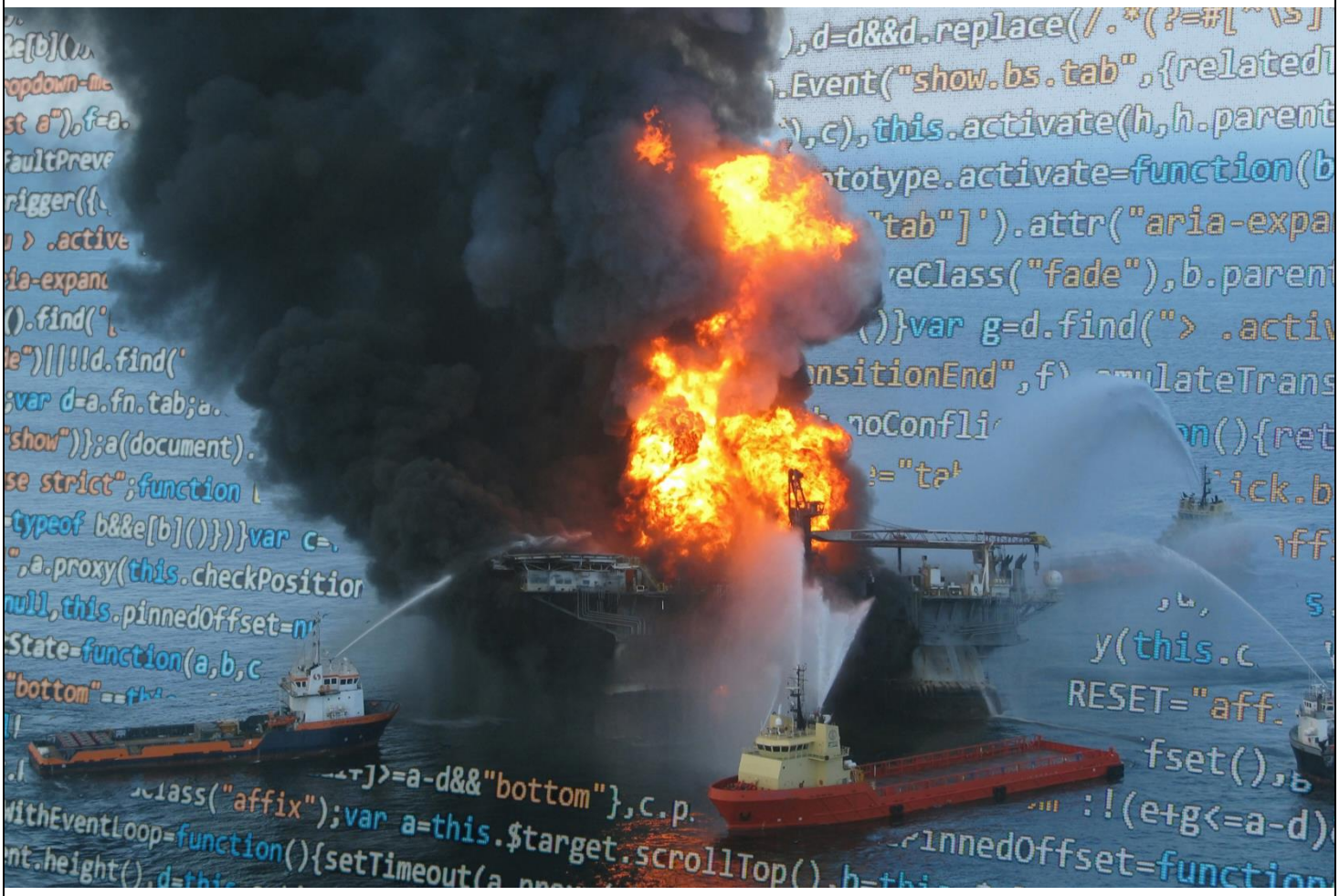
L'assurance des risques cyber

Gaspard Ferey, Nicolas Grorod, Simon Leguil

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

Année de soutenance : 2017

Gaspard FEREY Nicolas GROROD Simon LEGUIL

Pilote

Henri SERRES

Ingénieur général des mines, Membre associé du Conseil général de l'économie

Terrains

Alexis de BEAUREGARD

Head of Business Development Retail P&C, Axa Global P&C

Yves VERHOEVEN

Sous-directeur relations extérieures et coordination, ANSSI

Sommaire

Introduction

Les systèmes d'information se diffusent très largement dans les entreprises et les ménages. Ces derniers en deviennent presque « cyberdépendants », ce qui les expose au risque d'une indisponibilité ou d'un usage détourné de leurs systèmes d'information : ce sont les risques cyber qui peuvent être la conséquence d'accidents, d'erreurs ou être le fait d'un attaquant.

Assez récente, leur apparition a tout naturellement conduit au début des années 2000 à la commercialisation de nouveaux produits d'assurance. Globalement, le marché peine toutefois à décoller, un phénomène pour lequel de multiples interprétations cohabitent : le risque cyber est mouvant, potentiellement systémique, et les niveaux de sécurité sont interdépendants. Mais plutôt que d'entrer dans le débat de l'assurabilité du risque cyber, nous préférons parler concrètement.

Après un bref rappel des fondamentaux du cyber et de l'assurance (I), nous proposons un état des lieux de l'assurance des risques cyber (II) pour en identifier les améliorations possibles. En détaillant quelques scénarios qui décrivent l'impact potentiel du risque (III), nous montrons que le risque cyber peut mobiliser toutes les lignes de produits d'assurance. La bonne nouvelle est que l'assurance n'est pas rendue caduque par la transformation numérique. Toutefois, se placer en soutien de la numérisation des entreprises requiert une réflexion sur l'ensemble de ses services davantage que la création de produits isolés.

Pour répondre aux défis du numérique, nous proposons des outils à destination des entreprises (IV) en vue de définir leur besoin assurantiel et de faire le meilleur usage de l'assurance. Nous analysons ensuite ce qui est exigé de l'assureur en contrepartie pour répondre à ce besoin (V), notamment dans la révision de ses grilles d'analyse et de ses prestations, qui devront plus que jamais intégrer des services. Cela implique qu'il relève des défis organisationnels, techniques et juridiques (VI). Nous concluons sur le rôle que devrait selon nous jouer la puissance publique (VII) : nous ne pensons pas qu'il faille légiférer (assurance obligatoire, fonds de garantie). Nous préférons que l'État joue le rôle de tiers neutre et de confiance, pour contribuer à faire progresser la connaissance du risque et mettre en relation demandeurs et offreurs de services.

Le lecteur pressé retrouvera les principales idées résumées en encadré au début de chaque chapitre.

Le mot « cyber » bénéficie aujourd'hui d'une remarquable aura : apposez-le sur la couverture d'un quelconque ouvrage et ses chances de succès en seront considérablement augmentées. De ses processus et de son organisation interne à la conception et la distribution de ses produits en passant par sa communication, aucun des maillons de la chaîne de valeur de l'entreprise n'est susceptible d'échapper à la numérisation. Dès lors, les penseurs de cette transformation bénéficient très naturellement de nombreuses tribunes. De son côté, la presse économique ne manque pas non plus de conférer au mot tout l'écho qu'il mérite, enjoignant dirigeants, cadres et étudiants de tout poil de se lancer avec entrain dans la révolution sous peine de passer à côté d'une transformation majeure de leur temps.

Cyberdépendance

Force est de constater que l'imagination des entrepreneurs ne semble souffrir d'aucune limite pour simplifier, transformer et réinventer les usages de tous les acteurs de la vie économique en tirant parti des très larges potentialités offertes par les outils numériques. Nous devenons pour ainsi dire « cyberdépendants » au point d'avoir grand-peine à imaginer nous passer des bienfaits de la dernière révolution en date. Cela nous ramènerait à un scénario post-apocalyptique analogue à celui envisagé par Barjavel dans son roman *Ravage* [1] où l'électricité disparaît. Cette dépendance implique mécaniquement de multiples vulnérabilités en cas de dysfonctionnement des systèmes d'information : aux risques traditionnels contre lesquels les entreprises doivent se prémunir viennent désormais s'adjoindre des risques d'une nature différente, du moins par leur origine. Ce sont les risques cyber.

Les développements qui suivront auront en partie pour objet de donner davantage de substance au concept de risque cyber mais d'emblée il semble utile de le définir plus précisément :

> *Risque cyber : pour une personne morale ou physique, tout risque d'atteinte d'origine immatérielle à la disponibilité, la confidentialité, l'intégrité ou la traçabilité de son système d'information.*

Cette définition demeure volontairement large et abstraite car les outils numériques se diffusent aux endroits les plus inattendus de la vie des entreprises. Souvent bien au-delà de l'imagination de leurs concepteurs, l'idée des outils précédant celle de leurs usages. Ainsi le risque cyber est-il par nature mouvant et ne connaît-il d'autres limites que celles qui s'imposeront à la diffusion des systèmes d'informations. Profitons de cette occasion d'ôter au risque cyber sa connotation souvent exclusivement malveillante en soulignant que les entreprises auront souvent à pâtir des conséquences d'accidents ou d'erreurs.

On discutera sans parvenir à s'accorder du degré de conscience des risques induits par les systèmes d'information au moment où les décideurs choisissent de les adopter. Gageons toutefois que malgré d'abondantes mises en garde [2], la volonté d'exploiter au plus vite les opportunités économiques portées par les nouveaux usages continuera de précéder de loin les préoccupations autour de leur sécurité et de leur résilience. Les cycles de développement s'accélérant et la pression pour être le premier à mettre les produits sur le marché s'accroissant, cet ordre des priorités ne semble pas avoir de raisons de changer à court terme. Notamment, le risque cyber possède cette caractéristique fondamentale d'avoir des causes et parfois des manifestations intangibles, lui conférant un caractère intrinsèquement abstrait. Au premier abord, il jouit donc naturellement d'une visibilité moindre que les risques matériels, corporels ou financiers.

Le risque cyber s'insinue souvent sous les radars des entreprises et surtout des usagers de leurs produits ou services et d'aucuns n'hésitent pas à prédire qu'il sera à l'origine de la future crise d'ampleur comparable à celle des *subprimes*[1]. Cela n'empêche pas les lanceurs d'alerte de bénéficier d'une médiatisation croissante. Ils attirent l'attention sur le fait que la baisse des coûts et l'interconnexion ont également profité aux acteurs malintentionnés qui sont désormais techniquement en mesure de toucher des cibles en tout point du globe. Les récits de sinistres d'origine cyber fleurissent ainsi dans la presse[2], même si leur impact tangible reste souvent très difficile à mesurer. Au moins dans les grands groupes, à défaut d'une compréhension fine des véritables enjeux économiques du risque cyber, la prise de conscience progresse et naturellement avec elle, la volonté de remédier aux conséquences potentielles d'un scénario d'origine immatérielle.

---

[1] Au sens où elle serait la conséquence de l'explosion au grand jour d'un risque que les acteurs économiques auraient accepté de prendre en accordant une attention quasi exclusive aux bénéfices économiques de court terme au détriment d'une approche prenant en compte les risques sur la stabilité à un horizon plus lointain de la logique de fonctionnement instaurée.

[2] Une des dernières de grande ampleur est l'attaque *Wannacry* qui a touché 200 000 organisations dans plus de 150 pays, essentiellement des entreprises, chiffrant une partie de leurs données (selon Rob Wainwright, le directeur d'Europol, dans des propos rapportés par *Le Monde*).

L'assurance ne résiste pas à l'engouement cyber

À la demande de leurs clients mais aussi parce qu'ils y voyaient une opportunité de croissance, les assureurs, partenaires historiques du développement et de la résilience des entreprises, ont commencé à réfléchir puis à proposer des solutions indemnitaires. Un marché de l'assurance des risques cyber est donc né, d'abord aux États-Unis à partir des années 2000 et plus récemment, en Europe continentale et notamment en France. Ainsi en 2016, les primes collectées sur le marché mondial de l'assurance des risques cyber représentaient environ 3 milliards de dollars. Rapporté au total de l'assurance non-vie (1300 milliards de dollars de primes collectées en 2016), cela en fait un marché de taille relativement modeste.

L'assurance n'est toutefois pas épargnée par l'agitation qui règne autour du cyber et, au-delà de la multiplication des attaques, plusieurs éléments viennent corroborer l'hypothèse selon laquelle le marché pourrait connaître une croissance substantielle dans les années à venir. Au premier rang, l'entrée en vigueur du Règlement Général sur la Protection des Données (RGPD) en mai 2018, un texte européen qui précise les responsabilités de toutes les entreprises qui détiennent ou manipulent des données à caractère personnel et fait peser sur les coupables de défauts de traitement la menace d'amendes pouvant s'élever à 4% de leur chiffre d'affaires mondial, ou 20 millions d'euros, en sus des éventuelles réparations qui pourraient également atteindre des montants considérables puisque la porte serait ouverte à des actions collectives.

Tous connectés mais pas encore concernés

Plus généralement, la diffusion d'outils de prévention embarquant des logiciels et éventuellement connectés, des détecteurs de fumée aux systèmes de sécurité embarqués, permettent certes de faire baisser la sinistralité. Il n'est toutefois pas exclu qu'ils connaissent des dysfonctionnements de nature informatique voire qu'ils soient détournés à distance de leur usage, ce dont leurs fabricants pourront être tenus responsables. La diffusion de ces systèmes à un large panel d'usagers va probablement engendrer un glissement de la responsabilité générale, personnelle, vers une responsabilité « cyber », des fournisseurs.

On a donc vite fait de promettre l'assurance des risques cyber à un avenir radieux et ce, avant même de s'être interrogé sur la nature des garanties offertes par les produits qu'elle désigne. En effet, si l'on imagine aisément ce qu'être assuré contre la destruction d'un immeuble signifie, on éprouve une plus grande difficulté à se représenter la réalité que recouvre le fait d'être assuré contre les risques cyber. C'est probablement ce flou qui a contribué à ne pas en faire la priorité de certaines

entreprises, venant retarder le décollage du marché. De même, la nature mouvante du risque cyber et leur manque de maîtrise technique auront pu dans une certaine mesure tempérer l'appétit des assureurs. Ces derniers y voient également un risque potentiellement systémique : du fait de la diffusion ubiquitaire des outils numériques, ils pourraient être à l'origine de catastrophes touchant un nombre considérable d'acteurs économiques, portant les indemnisations à des niveaux qui menaceraient la résilience des souscripteurs.

L'éternel débat de l'assurabilité

Une littérature abondante [3] [4] [5] examine les raisons qui pourraient faire échouer le marché de l'assurance des risques cyber : asymétries d'information, niveaux de sécurité interdépendants et faibles incitations à l'investissement, fortes corrélations entre les profils des acteurs et difficulté à les discriminer selon leur niveau d'exposition au risque pour ne citer que les arguments les plus récurrents. Une des caractéristiques les plus frappantes du débat opposant promoteurs et détracteurs de l'assureur des risques cyber est sa capacité à émerger sur un objet que nous peinons encore à définir de manière pertinente.

Alors, plutôt que de nous prononcer ou de chercher à identifier des verrous au développement du marché, avec la certitude de pouvoir proposer une lecture de son évolution future qui vienne corroborer notre proposition, nous préférons faire œuvre de pragmatisme et réfléchir aux moyens que l'assurance au sens large pourrait déployer pour se mettre au service de la résilience des entreprises qu'elle accompagne, dans un contexte de numérisation intensive de leurs outils, produits et services.

Les scénarios : un outil de diagnostic et de recommandation

Pour ce faire, nous souhaitons parler concrètement et sur la base d'un outil qui nous semble clé dans la capacité des assureurs et des entreprises à envisager les solutions adaptées : des scénarios décrivant des sinistres d'origine immatérielle. Ces scénarios ont la triple vertu de permettre l'identification des actifs et processus critiques dans l'activité d'une entreprise, de fournir une base de discussion pour la quantification de leurs conséquences et d'apporter les bases budgétaires pour bâtir les stratégies d'arbitrage entre réduction et transfert de l'exposition au risque. Ils nous permettront notamment de montrer que les impacts des risques cyber sont potentiellement beaucoup plus larges que ne le laisse entendre le format actuel des produits d'assurance dédiés et que l'indemnisation des conséquences d'un sinistre

d'origine immatérielle ne se fera parfois à un niveau adéquat qu'au prix de la mobilisation de l'ensemble des couvertures assurantielles, dont les plus classiques.

Du point de vue de l'assurance donc, le « cyber » ne semble pas constituer une nouvelle catégorie autonome de risques et le concept d'un produit unique « assurance contre les risques cyber » n'est pas en soi pleinement satisfaisant. La bonne nouvelle pour l'assurance est qu'elle n'est pas rendue caduque par la révolution numérique, toutefois elle ne pourra pas prétendre la soutenir utilement si elle fait l'économie d'une réflexion globale sur son offre. Nous proposerons des pistes qui permettront un dialogue entre assureurs et entreprises en vue de faire émerger les solutions adaptées, et verrons comment l'État, notamment en jouant le rôle de plateforme, pourra se placer en soutien de ces transformations.

Précisons enfin que ce mémoire a été l'occasion de consulter de nombreux acteurs dans les compagnies d'assurance, de réassurance et de courtage, dans les entreprises, chez les éditeurs de solutions et prestataires de cybersécurité, ainsi que dans les institutions qui possèdent des groupes de travail touchant à son sujet. Nous profitons de cette occasion pour les remercier de l'accueil qu'ils nous ont réservé et espérons que la synthèse de leurs discours respectifs que nous proposons ici contribuera modestement à faire progresser leur réflexion.

I. Préambule : de quoi parle-t-on ?

En bon néophyte, lancez les mots « risques cyber » au détour d'une conversation entre spécialistes de la gestion du risque. Avant même d'avoir eu le temps de poser son objet vous donnerez lieu à coup sûr à un débat passionné. Certains déploreront la frilosité des assureurs qui refusent de garantir les actifs immatériels des entreprises, d'autres prédiront que l'horizon auquel chacun d'entre nous sera coté en bourse n'est pas si lointain et les derniers prophétiseront la chute des grands noms de l'assurance, précipitée par l'action des géants d'Internet. Désemparés face à cet abîme de complexité, vous peinerez à vous forger votre propre opinion du problème en apparence simple de la définition d'une réponse assurantielle à la transformation numérique. Nous proposons ici de définir simplement les deux objets que nous manipulerons : l'assurance et les risques cyber.

Quelques caractéristiques-clés de l'assurance

L'idée à la base de l'assurance est simple : des personnes physiques ou morales désirant réduire leur exposition aux conséquences d'événements jugés aléatoires mutualisent une partie de leurs capacités financières en vue d'être indemnisées en cas de survenance d'un sinistre. Si les risques garantis satisfont une série de conditions de nature probabiliste que nous décrirons brièvement dans la suite, alors plus les parties prenantes d'un groupe de mutualisation sont nombreuses, plus l'exposition globale est prévisible et le dispositif collectivement efficace.

Un objet aux origines lointaines

L'histoire fait remonter la naissance de mécanismes de mutualisation des risques à la haute antiquité, au moment où des commerçants étaient exposés à l'éventualité du pillage de leurs caravanes. Ces modèles d'assurance restaient archaïques et l'essor de l'assurance dans une forme proche de celle qu'on lui connaît aujourd'hui se serait produit avec le développement du commerce maritime sous les Grecs, naturellement exposé au risque de naufrage des navires marchands et avec lui, de la perte de cargaisons entières. Depuis, restant fidèle à ses principes fondateurs mais sans cesse contrainte de se réinventer, l'assurance a permis de libérer l'énergie de marchands, de travailleurs, d'innovateurs et d'industriels, ouvrant la voie à des réalisations totalement inédites. Henri Ford alla même jusqu'à dire : « New York n'est pas la création des hommes, mais celle des assureurs ».

Cependant, et c'est assez habituel avec l'assurance, la matérialisation des risques et les premiers sinistres précèdent l'émergence du marché d'assurance correspondant.

Le calcul du coût des prestations d'assurance repose en effet sur des bases actuarielles : c'est à la lumière de l'historique des pertes passées que l'exposition future est estimée, ce qui permet à l'apporteur de couverture de déterminer le niveau des primes qu'il doit collecter auprès des demandeurs. Cette précision est utile quand on constate que la conscience de la menace cyber est bien établie alors que le niveau de couverture assurantielle est susceptible de progrès significatifs.

L'assuré et un tiers à l'assuré : dommages et responsabilité

On distingue classiquement deux types de lignes d'assurance. Les assurances de personnes couvrent les atteintes à la vie et à la santé de l'assuré. Les bénéficiaires en sont l'assuré ou des tiers qu'il a désignés *a priori*. Les assurances de biens et de responsabilités quant à elles couvrent les dommages aux biens matériels et immatériels de l'assuré ainsi que les dommages, éventuellement corporels, causés à des tiers du fait de l'assuré. Des exemples simples de risques dont les conséquences peuvent être couvertes par des polices d'assurance sont l'incendie, le dégât des eaux, l'accident automobile, le bris de machine. Dans ce mémoire, les assurés seront surtout des entreprises, de sorte que les dommages subis directement par ces dernières occuperont une place importante et que les seules atteintes à la vie ou à la santé couvertes seront celles causées aux tiers à l'entreprise du fait de la poursuite de sa raison sociale.

Un assuré ne choisira habituellement de souscrire une police d'assurance couvrant les dommages qu'il cause à autrui que s'il en tenu responsable par la loi et que cette dernière exige qu'il en prenne en charge la réparation. Le droit de la responsabilité contribue donc à délimiter le champ des possibles pour les polices d'assurance. Au gré de la judiciarisation et de la contractualisation croissante des relations entre agents économiques, plus récemment, des contrats couvrant la responsabilité des dirigeants d'entreprises, ou la responsabilité du fait de leurs produits ou en cas d'erreur, d'omission ou de défaut de service, sont venus enrichir le panel des couvertures offertes. Les dommages couverts ne sont donc pas nécessairement matériels ou corporels mais peuvent être immatériels, de nature financière (une perte de marge du fait d'une interruption d'activité) ou plus abstraite (un préjudice moral, auquel cas l'indemnisation sera le plus souvent de nature financière). On distingue classiquement les dommages immatériels selon qu'ils sont consécutifs ou non à un sinistre matériel ou corporel.

On peut schématiser à grand trait les couvertures assurantielles à la disposition des entreprises dans le tableau suivant :

	Dommages assurables	Exemples
Dommages de l'assuré	Dommages matériels	Destruction d'immeubles, bris de machines
	Pertes financières directes	Remboursement de fonds détournés
	Pertes d'exploitation	Perte de recettes, frais supplémentaires d'exploitation
	Frais de gestion de crise	Frais de recherche de cause, d'expertise
	Frais liés à la sauvegarde de la réputation	Frais exceptionnels de communication
	Protection juridique	Conseil et assistance juridique
Dommages causés à des tiers (responsabilité)	Dommages matériels aux tiers	Frais de réparation de fenêtres brisées chez des riverains après une explosion d'un site industriel
	Dommages immatériels consécutifs	Perte de revenus lors d'une hospitalisation du fait d'une blessure causée par l'assuré
	Dommages immatériels non-consécutifs	Perte de recettes du fait d'un dysfonctionnement d'un logiciel fourni par l'assuré
	Dommages corporels	Frais d'hospitalisation d'un passant renversé par un salarié dans l'exercice de ses fonctions
	Frais de retrait - dépose - repose	Frais de remplacement chez un client d'une machine défectueuse
	Défense recours	Frais d'avocats engagés en cas de contentieux
	Responsabilité des mandataires sociaux	Indemnités de licenciement en cas de baisse d'activité consécutive à une erreur de gestion manifeste

Tableau 1 : Grandes lignes de produits d'assurance à disposition des entreprises.

En vue de protéger les consommateurs, l'activité d'assurance est réglementée. La loi du 13 juillet 1930 sur les assurances des véhicules terrestres à moteur a posé les bases du droit des assurances, qui sera codifié le 16 juillet 1976. Les assureurs jouent

également un rôle important dans la résilience de l'activité économique de sorte que leur solvabilité doit être assurée. Les compagnies se conforment en France à des exigences réglementaires sur leur niveau de capitalisation, aujourd'hui fixées au niveau européen par une directive (dite « Solvabilité II » dans sa dernière mouture).

Les conditions classiques d'assurabilité

Il existe plusieurs conditions jugées nécessaire au développement d'un marché d'assurance sain et durable qui tiennent à la nature des risques couverts et aux comportements des assurés face à l'éventualité de leur réalisation.

Pour synthétiser, classiquement, un risque sera assurable s'il est aléatoire [3], suffisamment courant pour offrir des bases actuarielles solides, futur, involontaire et bien défini. Le caractère bien défini renvoie au fait que le contrat d'assurance doit contenir le moins d'ambiguïté possible quant aux lieu, temps et cause que les conditions de survenance du sinistre doivent vérifier pour déclencher une indemnisation et être suffisamment spécifique pour déterminer le périmètre de cette dernière. Bien sûr, la catégorie des risques assurables n'est pas figée et il n'est pas à exclure que des risques y entrent ou en sortent au gré des évolutions technologiques, mais également réglementaires. Seuls les risques licites seront ainsi assurables : la loi prévoit que les conséquences de condamnations ou d'amendes pénales ne pourront pas être assurées.

Le caractère involontaire de la survenance d'un sinistre renvoie à la notion d'aléa moral : la souscription d'un contrat d'assurance ne devrait pas induire des modifications du comportement de ses bénéficiaires au motif que ces derniers pourraient souhaiter son déclenchement. Toutefois, on hésitera moins avant de se rendre chez un médecin si l'on détient une assurance maladie et les bénéficiaires d'un contrat d'assurance vie pourront souhaiter la disparition de son détenteur. Un risque assurable est donc souvent un risque que l'on répugnera à voir se produire,

[3] Le caractère aléatoire est exploité si l'on construit de larges bases d'assurés indépendamment mais comparablement exposés au risque. La catégorie des risques assurables n'est donc pas figée : à mesure que le développement et la diffusion des technologies d'acquisition et de traitement des données viennent renforcer les capacités d'anticipation de sinistres, le champ recouvert par la notion d'aléa se restreint. Heureusement pour les acteurs du monde de l'assurance, de nouveaux usages se développent et avec eux, de nouveaux besoins de couverture.

par contraste avec certains risques de nature spéculative, comme peuvent l'être des projets d'investissement.

Dans certains cas, comme celui des catastrophes naturelles ou du terrorisme, il peut arriver que le besoin de couverture soit réel mais que seules certaines conditions d'assurabilité soient vérifiées, de sorte que l'appétit des assureurs ne permet pas de satisfaire la demande. L'État peut alors intervenir en couvrant directement les sinistres ou en offrant sa garantie aux assureurs qui choisiraient de souscrire ces risques. Des modifications du droit peuvent en outre venir modifier les mécanismes incitatifs qui s'appliquent aux assurés (comme le code de la route).

À la base des prestations d'assurance, le principe indemnitaire

Un principe clé sous-tend la majorité des prestations d'assurance par mutualisation[4] : leur caractère indemnitaire. Ce principe vient entériner le fait qu'afin d'éviter les dérives spéculatives, la couverture assurantielle a vocation, lors de la survenance d'un sinistre, à replacer l'assuré dans les conditions dans lesquelles il se trouvait avant le sinistre (sous-entendu ni moins, mais surtout ni plus). Tout contrat d'assurance dont le déclenchement dans certaines conditions pourrait conduire à un enrichissement de ses bénéficiaires serait vraisemblablement réputé illégal.

Des contrats prévoient le versement de prestations de nature forfaitaire ou paramétrique. Les remboursements de frais médicaux sont souvent forfaitaires, ce qui permet de s'affranchir de frais d'expertise et d'inciter les assurés à se tourner vers des prestataires réglementés ou qui satisfont à certains critères de compétence ou de compétitivité. Dans le cas paramétrique, le montant des prestations dépend de la valeur mesurée de certains paramètres lors de la survenance d'un sinistre, par exemple la vitesse du vent ou la pluviométrie s'agissant des catastrophes naturelles. Les solutions forfaitaires et paramétriques présentent le double avantage de définir le niveau des prestations de manière indiscutable et de permettre leur versement dans un délai réduit. Ces caractéristiques ne doivent pas éclipser le fait qu'elles sont calibrées sur un niveau jugé raisonnable ou vraisemblable des coûts et dommages subis par l'assuré de sorte qu'elles obéissent indirectement au principe indemnitaire.

---

[4] Par définition, l'assurance par capitalisation, dont l'assurance-vie est en France l'archétype, ne repose pas sur des bases indemnitaires.

Des solutions au manque d'appétit

La mutualisation n'a d'intérêt que si l'exposition des assurés au risque est suffisamment peu corrélée de sorte que la probabilité qu'ils viennent tous à subir un sinistre comparable dans un laps de temps court est très réduite. À ce titre, la qualité d'un portefeuille d'assurance dépend de sa diversification, qui peut résulter de la variété des risques couverts mesurée selon divers critères comme leur périmètre géographique, leur secteur d'activité économique ou encore leur âge s'il s'agit d'individus.

Il est utile de noter que l'intervention de l'État n'est pas la seule manière de faire face aux limites de l'assurabilité. Toutefois, les alternatives à l'assurance demeurent d'une diffusion plus confidentielle. Par exemple, l'asymétrie d'information est parfois trop importante entre assureur et assuré. Cela peut être le cas d'entreprises qui cherchent à assurer certains de leurs actifs sur la nature et la gestion desquels ils doivent maintenir le secret. L'assureur n'est alors pas en mesure de se prémunir du phénomène d'anti-sélection : ceux qui sont les moins prévenants sur la gestion de leurs actifs ont aussi le plus grand intérêt à acheter une couverture, de sorte que les primes exigées décourageront les acteurs qui portent un risque plus faible que la moyenne. Si leur taille le leur permet, ces derniers chercheront à mutualiser les risques en interne, via des structures appelées captives.

Dans certains cas, l'assureur ne bénéficiera pas des données suffisantes pour estimer son exposition à un certain risque et ne souhaitera pas porter individuellement des contrats en indemnisant les conséquences. Cela peut être le cas pour un risque rare. Un demandeur de couverture pourra toutefois trouver des moyens de se couvrir en échangeant directement ou par l'intermédiaire de l'assureur une partie de son exposition avec un autre acteur, soumis à moins d'obligations réglementaires ou obéissant à une saisonnalité différente (souvent plus longue, la période de révision des contrats d'assurance étant annuelle). Cet échange, devenu courant dans le cas des catastrophes naturelles, se fait par exemple sur le marché obligataire. Des produits dérivés sur le risque de défaut porté par les bailleurs de fonds (le risque de crédit) ont aussi connu un essor spectaculaire dans les mois qui ont précédé la crise financière de 2008.

Une garantie aux bienfaits multiples

Classiquement, au-delà de la réduction de l'incertitude, la recherche d'une couverture d'assurance a plusieurs impacts positifs pour corollaires. Sur le plan économique, elle aide à la création d'entreprises, notamment dans les domaines où

les entrepreneurs possèdent du fait d'un certain régime légal ou réglementaire une responsabilité vis-à-vis de tiers, des salariés victimes d'accidents du travail par exemple. Manquant individuellement de solidité financière pour faire face à un éventuel sinistre, l'assurance leur permet malgré tout de mener leur projet à bien. L'assurance est également un élément de la résilience et de la continuité de l'activité des entreprises : collectant les primes avant la survenance des sinistres, l'assureur est en mesure d'en indemniser les conséquences dans les meilleurs délais, avec la garantie pour l'entreprise de voir son activité interrompue pendant une durée minimale.

Enfin, le niveau des primes collecté dépend de l'exposition individuelle des assurés de sorte que chaque effort fourni par l'un d'entre eux pour réduire la probabilité d'occurrence d'un sinistre fait baisser le montant des primes. S'il est capable d'identifier *a priori* des indicateurs fiables du niveau d'exposition individuel d'un demandeur de couverture, l'assureur peut moduler le niveau des primes payées par ce dernier selon ce qu'il anticipe être son degré d'exposition. Il incite ainsi à la mise en place de ce que l'on peut qualifier de cercle vertueux de l'assurance. Le système de bonus-malus pour l'assurance auto est un exemple simple de ce mécanisme incitatif.

Des acteurs-clés du marché de l'assurance : courtiers et réassureurs

En plus des compagnies d'assurance, le marché fait intervenir d'autres acteurs. Les courtiers jouent un rôle important dans la stimulation de la compétition entre les assureurs. Ils sont mandatés pour chercher dans le marché d'assurance une couverture définie par un agent qui cherche à s'assurer au meilleur prix. Sa plus-value provient de ses contacts multiples avec les assureurs dont découle son pouvoir de négociation et de son apparente neutralité face à la survenance des sinistres, en ce qu'il ne porte en théorie aucune exposition en propre. Dans la réalité, le courtier joue également le rôle de conseil, offrant à son client un support pour la caractérisation des risques auxquels il est exposé et la définition de la couverture adéquate.

Compte tenu de son implantation, une compagnie d'assurance peut détenir un portefeuille de risques dont le niveau de corrélation est élevé, mais pourrait être acceptable dans un groupe de mutualisation géographiquement plus large. Dans d'autres cas elle ne dispose pas des compétences pour traiter un risque sur le plan technique, par exemple si un sinistre est susceptible de toucher une proportion non-négligeable d'assurés avec des conséquences sur la solvabilité de l'assureur. Dans les situations précédentes, des opportunités de diversification existent mais l'assureur ne peut pas les exploiter à un coût commercial ou d'ingénierie acceptable. Il s'agit par

exemple des risques rares ou catastrophiques, comme les risques naturels. Un marché secondaire visant à exploiter des compétences techniques spécifiques ou à créer des bases de mutualisation plus larges possède dès lors tout son intérêt : il s'agit du marché de la réassurance, sur lequel les assureurs transfèrent à leur tour une partie de leur portefeuille. Les modalités de réassurance sont multiples mais schématiquement, dans les traités qui les lient aux réassureurs, les assureurs peuvent choisir de leur faire supporter une part proportionnelle ou contenue dans une tranche bien définie de leurs prestations.

Quels risques cyber ?

Le risque cyber est un concept qui recouvre de multiples réalités. Nous n'en ferons pas ici une description exhaustive mais chercherons à mettre en exergue celles de ses caractéristiques qu'il est important de garder à l'esprit lorsqu'on souhaite proposer des solutions assurantielles.

Avant de donner quelques exemples de sinistres cyber, rappelons la définition que nous en donnions en introduction :

> *Risque cyber : pour une personne morale ou physique, tout risque d'atteinte d'origine immatérielle à la disponibilité, la confidentialité, l'intégrité ou la traçabilité de son système d'information.*

Par système d'information on désigne l'ensemble des outils et processus qui permettent à l'entreprise de conserver, consulter, échanger ou manipuler des données dématérialisées. Précisons également qu'une atteinte au système d'information n'est pas obligatoirement d'origine malveillante, contrairement à une idée largement répandue.

Quelques exemples pour fixer les idées

L'atteinte à la disponibilité du système d'information d'une entreprise va souvent détériorer sa capacité à poursuivre son activité de manière normale. L'exemple le plus courant est celui du *ransomware*, un logiciel malveillant qui, une fois exécuté, va chiffrer une partie des données de la cible et en proposer le déchiffrement moyennant le paiement d'une rançon. La majorité des attaques cyber médiatisées auxquelles sont aujourd'hui sujettes les entreprises est de cette nature, les rançons venant alimenter les caisses d'organisations criminelles ou de groupes d'activistes. Selon le périmètre des données touchées, les conséquences peuvent varier d'anecdotiques (historique de messagerie interne) à financièrement substantielles et avoir un impact sur la capacité de l'entreprise à générer du revenu (données de

facturation future, base de clientèle). La disponibilité du système d'information peut également souffrir d'attaques dites en déni de service, dont la mécanique est de solliciter un nombre important de connexions aux services en ligne d'une entreprise, en vue de les saturer et d'empêcher les utilisateurs légitimes d'y accéder. Si c'est une plateforme de vente en ligne qui est visée les conséquences sur les recettes pourront être considérables.

Les informations détenues par l'entreprise peuvent susciter la convoitise pour leur intérêt commercial (base de données sur la clientèle) ou technologique (plans d'un produit ou code informatique d'un logiciel permettant de fournir des services). Certaines de ces informations pourraient venir à être diffusées par erreur ou acquises par un attaquant. Les conséquences pour l'entreprise sont de nature variable, pouvant aller de d'une détérioration de sa réputation auprès de ses clients (entreprises ou particuliers) et de ses fournisseurs à la perte d'un avantage compétitif, dans le cas où l'atteinte porte sur sa propriété intellectuelle.

Les atteintes à l'intégrité des données d'une entreprise sont plus subtiles mais n'en sont pas moins lourdes de conséquences. Elles sont aussi bien le fait d'erreurs et d'omissions (modification involontaire ou sauvegardes incomplètes) que d'actes malveillants (prise de contrôle de systèmes à commande informatique). Par exemple, une modification dans l'inventaire d'une entreprise pourra, s'il est sous-estimé, mener à des commandes générant des excédents et venant augmenter artificiellement le besoin en fonds de roulement. La prise de contrôle d'un moyen de production pourra, dans les cas les moins graves conduire à un arrêt de l'activité et dans les plus graves, à des dommages matériels et corporels (voir les exemples présentés dans les scénarios de la partie III. Du concret : scénarios de sinistres).

Sur le plan technique, la traçabilité est plus difficile à établir et à préserver mais elle est déterminante dans la réputation dont jouissent certains acteurs auprès de leur écosystème de clients et de fournisseurs. La traçabilité revient à la capacité à tenir un registre de l'ensemble des connexions et modifications apportées à un système d'information. Par exemple, les agents et établissements qui sont dépositaires d'un historique de transactions, immobilières pour les notaires, financières pour les banques, se doivent d'en garantir la traçabilité en vue d'éviter la répudiation des contrats qu'ils ont contribué à conclure, de manière plus ou moins explicite. Leur activité repose en premier lieu sur la confiance des tiers dont ils manipulent les données, cette dernière étant maintenue au prix de leur capacité à conserver un historique indiscutablement fiable des transactions qu'ils ont contribué à conclure.

Ces quelques exemples démontrent le point auquel les entreprises ont accru leur dépendance aux systèmes d'information. D'une part ils sont indispensables aux opérations internes : acquisition, conservation, exploitation des données, communication entre les employés mais également contrôle et asservissement des systèmes de production pour les entreprises concernées. D'autre part, ils contribuent à créer des interfaces entre l'entreprise et les acteurs dont son avenir dépend : clients dont particuliers, fournisseurs, mais aussi médias, concurrents ou institutions, dont les états.

Du point de vue de l'assurance, il est utile de souligner trois conséquences de cette dépendance.

La première tient au degré d'interconnexion des acteurs économiques, qui au passage a permis le partage de la valeur sur des chaînes d'une longueur et d'une complexité toujours croissantes. Les entreprises dépendent aujourd'hui des flux d'information qu'elles échangent, de manière standardisée et en utilisant des solutions proposées par un nombre restreint de fournisseurs. Cette standardisation implique qu'un dysfonctionnement, d'origine malveillante ou non, peut toucher directement et identiquement un nombre important d'acteurs. L'interconnexion implique quant à elle que l'incapacité d'un acteur à disposer pleinement de ses moyens peut avoir des conséquences sur les nombreux autres agents qui dépendent de lui. Aux yeux de l'assureur, le risque cyber possède donc dans certaines de ses manifestations tous les attributs d'un risque systémique : un sinistre pourra donner lieu à des indemnisations simultanées chez un nombre important d'acteurs, avec un risque pour sa propre solvabilité.

La deuxième conséquence est que, manifestement, le système d'information d'une entreprise est un objet dont le périmètre est de plus en plus flou. Les données de l'entreprise sont accessibles à ses employés en tout point du globe grâce à leurs smartphones, le cas échéant, le code informatique qu'elle a mis au point est exécuté dans chacun des produits qu'elle distribue et internet lui offre une vitrine commerciale potentiellement mondiale. Signe d'opportunités économiques décuplées, ce caractère ubiquitaire des systèmes d'information implique également un accroissement du périmètre de responsabilité de l'entreprise, créant une complexité qu'elle peine à gérer. La surface d'attaque n'a plus pour limite que l'imagination des acteurs malveillants, potentiellement extrêmement motivés et dans bien des cas très difficiles à identifier car jouant de mécaniques complexes. Dans certains cas, ces caractéristiques apparaîtront comme autant de limites aux

caractères aléatoire et bien défini du risque cyber, et par conséquent à son assurabilité.

Enfin, la numérisation massive a provoqué une contraction des échelles de temps à plusieurs égards. D'abord dans le rythme d'échange des informations, venant accroître d'autant l'impact potentiel de leur indisponibilité et des pertes d'exploitation qui s'ensuivent. Ensuite dans la nécessité, une fois survenue, de gérer une crise dans les plus brefs délais car une information erronée ou nuisible à l'image de l'entreprise est susceptible de se propager très rapidement, de même qu'une brèche dans la confidentialité ou l'intégrité de ses données. Nous aurons l'occasion d'insister à nouveau sur cette dimension temporelle du risque cyber quand nous évoquerons la nécessité pour l'assureur d'adapter son offre en vue d'y inclure davantage de services, à la fois de prévention, de gestion de crise et de remédiation.

Le règne de l'intangible

Les transformations impliquées par la révolution numérique sont loin de se cantonner à celles que nous venons de décrire. Nous ne prétendons pas en dresser un portrait exhaustif mais souhaitons attirer l'attention sur un dernier élément récurrent dans les débats sur le rôle qu'a à jouer l'assurance.

Il s'agit de la part croissante de son capital informationnel dans la valeur actuelle et future d'une entreprise. Au gré des vagues successives de dématérialisation, la conservation et la manipulation de ce capital repose de plus en plus sur les systèmes d'information. D'aucuns argueront que cette information possède une réalité physique et matérielle car elle est codée dans des disques durs par des *bits* dont la valeur est définie par le sens d'un champ magnétique. Nous ne pensons pas que ce soit essentiel dans la mesure où cette réalité physique ne préjuge en aucune manière la valeur intrinsèque de l'information.

La conséquence pratique du stockage et de la manipulation de la donnée par les systèmes d'information est son accessibilité et détention éventuelle par un agent physiquement extérieur à l'entreprise. À trop insister sur le caractère matériel de la donnée, on pourra également passer à côté d'une des caractéristiques clés : celle de pouvoir être détenue par plusieurs personnes en même temps et de manière difficilement traçable.

La part croissante que les données représentent dans leur valeur actuelle et future n'a pas échappé aux entreprises. Certaines d'entre elles, dont l'avantage compétitif repose sur une propriété intellectuelle farouchement défendue, peuvent chercher à souscrire auprès des assureurs des polices les couvrant dans l'éventualité où elles

verraient certaines de leurs informations dérobées. Nous comprendrons dans la suite qu'au-delà des difficultés inhérentes au chiffrage des préjudices subis au titre de la perte de confidentialité de données, l'idée de leur indemnisation serait susceptible de contrevenir aux bases indemnitaires qui sous-tendent les prestations d'assurance et de favoriser l'apparition de logiques de nature spéculative.

II. Bref état des lieux de l'assurance des risques cyber

Il existe aujourd'hui un certain nombre de couvertures assurantielles spécifiquement dédiées aux risques cyber et estampillées comme telles. Elles répondent majoritairement à un besoin de couverture face à des typologies de sinistres assez spécifiques apparues à la suite de la numérisation des activités économiques.

Elles s'adressent à des entreprises qui possèdent un fort niveau de dépendance à leur système d'information ou sont amenées à manipuler un nombre important de données dont la perte de confidentialité pourrait être dommageable à des tiers à l'entreprise, personnes morales ou physiques.

Ces couvertures possèdent des variantes selon qu'elles sont orientées vers les volets dommages ou responsabilité de l'assuré mais sont pour certaines empreintes d'une coloration anglo-saxonne, les premières ayant fleuri au début des années 2000 Outre-Atlantique. Elles offrent dans tous les cas un type de couverture bien spécifique centré autour de dommages bien identifiés : frais de gestion de crise, pertes d'exploitation et autres dommages immatériels non-consécutifs.

Les travaux récents de l'OCDE [6] dressent un portrait complet et exhaustif des polices dédiées à l'assurance des risques cyber qui sont aujourd'hui proposées sur le marché de l'assurance. Sous la forme d'un rapport d'étonnement, nous proposons ici de parcourir ce que nous semblent en être les caractéristiques essentielles afin d'en identifier les apports mais également les éventuelles lacunes.

La vérité sur les sinistres cyber

Aujourd'hui, la majeure partie des sinistres de nature cyber connus du public se répartissent en trois catégories :

- La divulgation involontaire ou le vol de données confidentielles, notamment de bases de données clients, à des fins commerciales mais aussi d'usurpation d'identité et de fraude bancaire. Les conséquences portent sur la réputation de l'entreprise mais aussi sur les tiers visés par des démarches commerciales agressives ou pécuniairement victimes des fraudes. Dans le cas où l'entreprise n'est pas seule propriétaire des données qu'elle détient, elle peut être amenée à réparer les conséquences auprès des tiers de leur perte de confidentialité.

- La demande de paiement d'une rançon, sous peine de divulgation d'informations confidentielles [5] ou de destruction/corruption de données critiques. La première touchée est l'entreprise, qui peut avoir des difficultés à poursuivre son activité et voir sa réputation touchée et surtout le potentiel de ses marchés futurs dégradé.
- Les attaques en déni de service, qui rendent indisponibles une partie des services en ligne de l'entreprise, en vue de faire pression sur elle. L'impact sur les recettes et la continuité d'activité est direct et touche plus largement la réputation de l'entreprise.

Fort de cette classification des sinistres, on comprend que la remédiation à leurs conséquences occasionne plusieurs types de pertes pécuniaires ou assimilables qui sont au moins pour partie susceptibles de faire l'objet d'indemnisations dans le cadre d'une police d'assurance.

- Le traitement des dommages subis par l'entreprise : il s'agit de faire cesser l'attaque ou la fuite de données, de s'assurer que l'éventuel attaquant est bien sorti du périmètre confidentiel du système d'information de l'entreprise, que le sinistre n'est pas susceptible de se reproduire à l'identique, et le cas échéant, de reconstituer les données de l'entreprise. La gestion de cette crise nécessite l'intervention coûteuse d'experts, souvent extérieurs à l'entreprise. En vue de sauvegarder son image, l'entreprise peut également devoir engager des frais exceptionnels de communication (spots publicitaires). Selon les obligations qui pèsent sur elle, l'entreprise devra notifier aux tiers la perte de confidentialité de données les concernant, ce qui nécessite d'identifier les personnes touchées, une démarche potentiellement coûteuse. Selon le droit applicable, l'entreprise pourra souffrir d'une amende de nature pénale ou administrative.
- La réparation des conséquences sur les tiers. Elles peuvent être directement financières en cas de fraude bancaire ou prévues sous la forme de pénalités contractuelles, par exemple en cas de perte de confidentialité de données.

[5] Les conséquences peuvent être très lourdes, comme dans le cas de l'affaire Sony en décembre 2014 au cours de laquelle des notes sur des scénarios de films aux budgets colossaux avaient été dévoilées.

Elles relèvent dans d'autres cas de la réparation de préjudices moraux[6], dont l'évaluation sur le plan financier dépend fortement du droit applicable. Au-delà du montant des réparations, l'entreprise peut également avoir à faire face à des frais de procédure légale et de défense.

- À la fois l'entreprise visée et des tiers peuvent subir des pertes d'exploitation au cours du sinistre. Ces pertes d'exploitation, s'il est possible de les relier directement au sinistre et d'en proposer un chiffrage, peuvent faire l'objet d'indemnisations.

Pour quelles solutions assurantielles ?

À l'exception des conséquences sur les opportunités et marchés futurs de l'entreprise qui découlent de la dégradation de sa réputation, les pertes précédemment décrites sont connues de l'assurance. Les scénarios cyber viennent simplement en modifier en partie la nature, par exemple pour les réparations auprès des tiers, ou l'ampleur, notamment pour les frais de gestion de crise (experts, communication) et de notification.

Avec l'essor des vols de données bancaires et d'identité survenu au début des années 2000 notamment aux États-Unis, s'est tout naturellement fait jour l'idée de proposer de nouveaux produits d'assurance adaptés à la typologie des sinistres. En raison d'un terrain légal propice aux actions collectives pouvant déboucher sur des réparations de nature punitive et donnant lieu quoi qu'il arrive à des frais légaux, les produits nord-américains se sont construits autour de leurs volets responsabilité civile. Pour des raisons historiques, l'indemnisation des conséquences de sinistres cyber a été également exclue des polices existantes en vue d'être regroupée dans les nouvelles polices spécifiques, dites *standalone*.

En Europe continentale, avec moins de place pour les actions collectives, et surtout des systèmes d'accès au crédit et de paiement par carte bancaire plus sécurisés, l'essentiel des conséquences d'un sinistre cyber est porté directement par l'entreprise : frais de notification, gestion de crise et communication. Par conséquent, l'offre assurantielle s'est structurée autour des dommages subis directement par l'entreprise. Les volets de responsabilité n'ont pas été systématiquement exclus des

[6] Par exemple, en juillet 2015, une partie de la base clientèle de l'agence canadienne de rencontres extraconjugales *Ashley Madison* avait été dérobée et divulguée par des pirates informatiques.

polices traditionnelles, ce qui vient également expliquer la taille plus réduite du marché des polices dédiées au cyber en Europe continentale.

Aujourd'hui, les primes collectées pour les polices spécifiques représentent mondialement un montant d'environ 3 milliards de dollars, dont 90% aux États-Unis. Il n'y a pas de consensus sur les prévisions de croissance de ce marché, mais pour les raisons historiques et d'opportunité que nous avons évoquées, nous ne pensons pas que le marché européen doive à terme présenter une structure calquée sur celle des États-Unis. À noter, l'indemnisation des pertes d'exploitation et de l'interruption d'activité (dommages immatériels non consécutifs dans la majorité des sinistres cyber) commence timidement à figurer dans les prestations prévues par les contrats d'assurance. Pour le moment, les pertes futures subies du fait de la perte de confidentialité de données restent du domaine de l'inassurable.

De part et d'autre de l'Atlantique, les assureurs cherchent également à intégrer une offre de services de prévention et de remédiation à leurs polices d'assurance. Sur le plan commercial, cette démarche a l'avantage de permettre de proposer une solution clés en main aux entreprises, ce qui prend tout son intérêt pour les plus petites d'entre elles. Elle représente également une opportunité pour l'assureur de développer son activité sur une chaîne de valeur plus longue et moins capitalistique que ne l'est la pure activité assurantielle.

Et quelle qualité de couverture ?

Le champ des couvertures offertes est dans les deux cas, extrêmement délimité et n'inclut que très rarement les éventuels dommages matériels subis par l'entreprise lors d'un sinistre cyber. Surtout, les polices spécifiques sont assorties de plafonds de couverture qui dépassent rarement 200 millions d'euros, un chiffre qui a pu dans certains cas avérés correspondre seulement aux frais légaux. Ces plafonds de couverture sont pour partie la conséquence d'un manque d'appétit des assureurs.

On peut dès lors s'étonner que dans la presse, des entreprises soient décrites comme étant « assurées contre le risque cyber » simplement parce qu'elles ont souscrit une police spécifique. Parfois, elles l'auront fait pour des raisons discutables : satisfaire un administrateur, une agence de notation ou présenter un certificat à un client. Le fait que l'on cherche des couvertures assurantielles contre le risque cyber témoigne cependant du chemin parcouru en direction de son traitement sur un pied d'égalité avec les risques traditionnels, après qu'il aura été longtemps ignoré ou relégué au rang de préoccupation purement technique ne nécessitant pas l'allocation de budgets dédiés.

Loin donc de nier l'intérêt de ces polices, il nous semble utile d'en souligner le caractère par nature parcellaire et d'insister sur le fait qu'elles ne peuvent en aucun cas dispenser une entreprise d'une réflexion globale sur son exposition aux risques cyber, en vue de garantir sa résilience et la continuité de son activité.

Des courtiers ardents négociateurs

Notons enfin que, sur le marché français, les couvertures classiquement offertes par les polices dédiées au risque cyber sont standardisées, du fait d'une politique commerciale dynamique chez certains courtiers qui parviennent à imposer leurs termes aux assureurs[7]. Cette concurrence profite aux clients qui voient baisser le niveau des primes, toutefois, elle structure le marché autour d'une certaine conception du risque cyber avec deux conséquences, l'une pour les assureurs, l'autre pour les assurés.

Les assureurs, en recherche de croissance, acceptent souvent des termes plus larges qu'ils n'y seraient enclins compte tenu de leur appétit au risque et de ce qu'ils envisagent pouvoir être les conséquences de sinistres cyber. Ils cherchent notamment à transférer une bonne partie de leur exposition (jusqu'à 80% selon les chiffres qui nous ont été communiqués) en réassurance facultative dont les conditions font peu de cas de la nature et donc du degré de diversification des portefeuilles. En l'absence de sinistres de nature catastrophique, le système tel qu'il s'est construit perdure, mais la confiance dans l'assurance pourrait se voir diminuée si certains assureurs manquaient à faire face à leurs obligations lors de la concrétisation d'un scénario de grande ampleur.

S'agissant des assurés, ces polices standardisées couvriront dans la limite des garanties offertes des pertes qui, selon les profils, seront susceptibles de menacer directement l'activité de l'entreprise (chez un opérateur télécom) ou s'avèreront anecdotiques (producteur industriel sans clients chez les particuliers). C'est sur l'incapacité de couvertures standardisées à répondre à l'ensemble des besoins des entreprises que nous souhaitons dans la suite attirer l'attention en nous appuyant sur des scénarios détaillés. Cela permettra également de commencer à dégager les caractéristiques d'une réponse assurantielle adaptée aux enjeux de la révolution numérique.

[7] La plupart du temps, ils sont plusieurs à se syndiquer pour couvrir le risque d'une entreprise.

III. Du concret : scénarios de sinistres

Au moment de chercher à identifier la possible réponse assurantielle à la numérisation intensive de l'activité économique, rien de tel qu'un discours concret qui s'appuie sur la base de scénarios de sinistres. Ces scénarios devront constituer la base du dialogue entre l'assuré et l'assureur.

Les scénarios viennent également démontrer que face à la numérisation, toutes les entreprises ne se ressemblent pas. Leurs profils de risque et l'impact d'un certain type d'attaque dépendent de leur secteur d'activité, de leur taille et de leur niveau de dépendance à leur système d'information.

Élément important : l'ensemble des couvertures assurantielles, dont les plus classiques, peut être mobilisé face à un sinistre de nature cyber, ce qui plaide en faveur d'une adaptation de la couverture existante aux conséquences de la numérisation davantage que pour une réponse séparée et standardisée. Bien sûr, des pertes non-assurables demeurent mais ne doivent pas occulter le fait que dans bien des cas, l'assurance se positionnera en soutien de la résilience de l'activité de l'entreprise.

Les chapitres suivants de ce texte seront consacrés à des recommandations aux parties prenantes du marché de l'assurance que sont assureurs, entreprises cherchant à s'assurer, fournisseurs de services dans le domaine de la cybersécurité et pouvoirs publics. Leur objet sera de décrire une démarche opérationnelle permettant d'identifier les modifications du besoin assurantiel impliquées par la numérisation et de donner des éléments de réorganisation pour y faire face. Nous proposerons un outil de base pour l'ensemble de ces acteurs : la réflexion sur des scénarios dimensionnants permettant de localiser les actifs et processus critiques et d'en assurer un niveau de résilience face au risque cyber qui soit en phase avec l'appétit au risque de l'organisation. Nous défendrons l'idée que ces scénarios ne sont que partiellement transposables d'une organisation à l'autre, qui sous-tend la thèse selon laquelle une police standardisée estampillée « cyber » ne saurait répondre au besoin de couverture de l'ensemble des entreprises.

Dans cette partie, nous souhaitons donner quelques exemples de scénarios. Au-delà de fournir une base concrète à la discussion qui suivra, cela nous permettra d'introduire l'idée selon laquelle l'impact d'un sinistre cyber sera susceptible de varier très sensiblement d'une entreprise à l'autre, selon son secteur d'activité, sa taille et la place que tiennent les systèmes d'information dans ses opérations.

Nous présentons six scénarios sous une forme harmonisée : une brève description de la situation de l'entreprise victime du sinistre d'origine cyber, son impact en termes de pertes (assurables ou non) et la manière dont ces pertes recoupent les couvertures assurantielles sous leur forme classique (présentée dans la partie I. Préambule : de quoi parle-t-on ?), augmentée d'une ligne de dommages dits « consécutifs à une violation de confidentialité » que sont essentiellement des frais de recherche des tiers à l'entreprise dont des données auraient pu être dévoilées et le cas échéant, de notification. Afin d'identifier les couvertures assurantielles les plus utiles, nous distinguons ces pertes par leur magnitude en les comparant au résultat de l'entreprise. Ces scénarios sont inspirés par nos discussions avec les experts de la gestion du risque en entreprise et en assurance et par les travaux du Cambridge Centre for Risk Studies - Risk Management Solutions [7]. Nous terminons cette introduction en reconnaissant modestement que le chiffrage des pertes est proposé sur des bases hypothétiques et serait probablement désavoué dans son détail par l'expérience. Il est proposé afin de fixer les idées en vue de la discussion qui suit.

Les résultats sont présentés sous la forme synthétique d'un tableau à la fin de ce chapitre (Tableau 2).

Scénario 1 : PME de vente en ligne

Le premier sinistre cyber touche une PME qui mène en ligne une activité de négoce : par le biais de son site internet, elle vend à des particuliers des biens achetés auprès de leurs producteurs ou de grossistes et travaille avec certains d'entre eux en flux tendu, notamment pour les produits frais. Les activités physiques qu'elle mène en propre sont la réception, le stockage, le conditionnement et l'expédition des marchandises. Elle dispose d'équipes d'achat, de marketing, de service auprès des consommateurs et de support, dont la maintenance de son site internet, qui constitue sa vitrine.

Pendant 24 heures, cette entreprise est victime d'une attaque en déni de service : des demandes de connexion illicites provoquent l'indisponibilité de son site marchand pour tout utilisateur légitime. Une fois l'attaque terminée, le service est interrompu pendant 48 heures supplémentaires, la durée nécessaire aux équipes du prestataire informatique dépêché sur place pour s'assurer qu'un scénario identique n'est pas susceptible de se reproduire et qu'aucun attaquant n'est présent dans le système informatique de l'entreprise.

Pendant les trois jours d'indisponibilité, le chiffre d'affaires est perdu puis l'activité reprend timidement (50% du volume habituel de ventes) pour se stabiliser à 90% du

niveau saisonnier habituel au bout d'un mois. Une partie du stock de produits périssables est détruit. Certains fournisseurs dont le site était le premier moyen de distribution entament des recours pour faire reconnaître la négligence de l'entreprise et obtenir réparation du préjudice subi au titre de leur perte de chiffre d'affaires.

Les pertes les plus importantes pour l'entreprise sont les pertes d'exploitation consécutives à l'indisponibilité et la baisse de fréquentation. Comparés au résultat, les frais de gestion de crise (experts) sont substantiels de même que les frais de défense dans le cadre des actions intentées par certains fournisseurs. Au chapitre des pertes non-assurables se trouvent essentiellement les frais d'amélioration du système informatique pour le rendre plus fiable.

Scénario 2 : PME de services informatiques

Une entreprise fournit des services en ligne de stockage sécurisé : elle héberge les données de plusieurs centaines d'entreprises dont certaines peuvent être jugées confidentielles. Ses activités physiques sont concentrées autour de la gestion et de l'entretien de ses serveurs qui contiennent les disques durs. L'entreprise possède également des équipes de développement qui s'attachent à fluidifier et sécuriser le service ainsi que des équipes en charge du marketing et de la communication auprès des clients. Malgré sa petite taille, l'entreprise dégage un résultat important grâce à la réputation dont elle jouit dans le milieu professionnel pour la fluidité de ses services et la disponibilité des équipes de développement.

En vue d'optimiser l'utilisation des ressources, une mise à jour est préparée par les équipes de développement et destinée à être testée dans un premier temps. Par erreur, un employé déploie la version de test sur les outils de production. Pour des raisons d'incompatibilité avec le matériel de stockage, le service est inopérant pendant 24 heures, le temps nécessaire au rétablissement du service précédent, l'installation de la mise à jour n'étant pas directement réversible.

Pendant la durée d'indisponibilité, des clients qui bénéficiaient de sauvegardes automatiques continuent à transmettre des données mais ne parviennent pas à y accéder, ainsi qu'aux données antérieures. Ces données nouvellement transmises s'avèreront avoir été perdues. Une cellule de crise est mise en place pour recevoir leurs demandes et les aider à fonctionner en mode dégradé.

Même si rien ne prouve que l'attaque ait été d'origine malveillante, des clients perdent confiance en l'entreprise et recherchent des solutions alternatives. Pour endiguer leur départ, l'entreprise communique de manière intensive, se sépare de

l'équipe responsable de la mise à jour malheureuse et prend le soin de revoir son organisation, ce qui lui coûte en fluidité et réactivité. L'essentiel de la clientèle est maintenu mais des procédures longues de plusieurs mois sont engagées par certains clients pour obtenir la réparation des préjudices subis (perte de données confidentielles et frais supplémentaires d'exploitation).

Ces réparations constituent la plus grosse part du préjudice subi par l'entreprise, de même que les frais juridiques engagés pour sa défense. La responsabilité des mandataires sociaux est engagée pour défaut d'organisation. Enfin, les frais supplémentaires induits par la gestion de la crise (communication notamment), sont de moindre ampleur. Les pertes non-assurables majeures sont celles dédiées à la réorganisation, au recrutement de nouvelles équipes et à la sécurisation du service.

Scénario 3 : Entreprise de la grande distribution

Une entreprise de grande distribution dispose d'une filiale française qui emploie plusieurs milliers de collaborateurs pour dégager un résultat de quelques dizaines de millions d'euros. Elle repose sur un ensemble de grossistes et quelques fournisseurs locaux et a pour activité physique le stockage, le conditionnement et la distribution de ses produits, via ses magasins ou un service de livraison à domicile. Outre les équipes en charge des enseignes physiques, elle dispose d'équipes d'achat et de marketing.

La gestion de ses stocks et commandes aux fournisseurs est automatisée et repose sur un logiciel dédié. Profitant d'une faille de sécurité dans ce logiciel, un attaquant exécute un code malveillant qui modifie les stocks de manière aléatoire, entraînant en quelques jours des commandes excédentaires et des ruptures sur de nombreux produits. Une partie des produits frais excédentaires doit être détruite.

Face aux multiples ruptures, les clients se détournent temporairement des magasins de l'enseigne qui parvient après quelques semaines à rétablir la fréquentation à 90% de son niveau saisonnier habituel, jouissant d'une clientèle majoritairement locale. Une semaine pendant laquelle les commandes sont effectuées manuellement est nécessaire à un inventaire complet. Pendant deux semaines, une équipe d'experts informatiques est déployée pour s'assurer de la fin de l'attaque et rétablir un service informatique de qualité. Seule une partie des produits excédentaires peut être retournée aux fournisseurs et certains d'entre eux, également victimes de la désorganisation induite, entament des procédures contre la filiale. Parmi eux, quelques-uns dépendent fortement de l'enseigne pour écouler leurs produits.

Les pertes les plus importantes tiennent à la destruction des excédents commandés. Les frais de gestion de la crise (experts informatiques) et les frais supplémentaires d'exploitation résultant de la désorganisation (recrutement d'intérimaires) sont également substantiels. Une partie des actions engagées par les fournisseurs débouche sur réparation et occasionne des frais de défense importants. La responsabilité des mandataires sociaux est engagée. Parmi les pertes non-assurables figurent des frais importants d'amélioration de la sécurité du système d'information.

Scénario 4 : Port de marchandises

Un port de marchandises emploie directement quelques milliers de manutentionnaires, pilotes et dockers et dégage un résultat d'une trentaine de millions d'euros. Ses activités physiques consistent en la réception, l'entreposage et l'expédition de marchandises transportées par bateaux ainsi qu'en l'entretien des installations (quais, grues et voies ferrées). Les autres activités sont majoritairement destinées à attirer du trafic supplémentaire et maintenir l'activité existante.

Un attaquant informatique parvient à accéder à une partie du système d'information de l'entreprise et à prendre le contrôle du logiciel partiellement automatisé de commande d'une grue. Alors qu'un conteneur est suspendu à une grue, il en provoque la chute sur le navire qui le transportait, blessant deux membres d'équipage et endommageant son pont. Le moteur d'avion transporté dans ce conteneur est détruit. Le service de déchargement est interrompu le temps que des experts s'assurent que la cause de l'attaque est éliminée, ce qui crée de l'attente à l'entrée du port et conduit certains transporteurs à dérouter leurs navires. La fréquentation n'est rétablie à son niveau habituel qu'après plusieurs mois.

Le propriétaire du navire demande réparation du préjudice subi par ses deux employés blessés ainsi que la réparation de son navire, en sus des pertes d'exploitation consécutives à son indisponibilité pendant le temps de la remise en état. L'entreprise qui possédait le moteur au moment de sa destruction en demande le remboursement et les transporteurs dont les marchandises ont été immobilisées ou déroutées demandent réparation de leurs frais supplémentaires d'exploitation.

Le niveau des pertes liées aux préjudices subis par des tiers est considérable par le montant des réparations et les frais juridiques engagés. Le port subit des pertes d'exploitation liées à l'interruption d'activité, aux frais supplémentaires et à la baisse temporaire de la fréquentation. Le port doit également faire face à des frais de remise en état de la grue et des dépenses supplémentaires liées à la gestion de la crise (experts informatiques).

Au rang des pertes non assurables, certains contrats avec des clients incluaient des pénalités de retard qui ne peuvent être couvertes par l'assureur en raison de leur montant d'ordre punitif.

Scénario 5 : Entreprise de médias

Une entreprise de médias emploi quelques milliers de collaborateurs et dégage un résultat d'une centaine de milliers d'euros. Ses activités vont de la production de contenu (programmes d'information, séries télévisées, longs métrages) à la vente de produits déclinés à partir des contenus diffusés. Même si la majeure partie de son chiffre d'affaires provient de ses recettes publicitaires, la diversité des collaborateurs qu'elle emploie reflète celle de ses activités. Une grande partie de l'infrastructure de production, stockage et diffusion de contenu étant dématérialisée, l'entreprise est hautement dépendante de la disponibilité de son système d'information.

Un intrus dans le système d'information parvient à en exfiltrer des données confidentielles et en diffuse une partie. Il demande le paiement d'une rançon sous peine de les diffuser en entier. Ces données sont de plusieurs natures : scénarios de productions futures et contrats publicitaires. L'entreprise fait intervenir en urgence des prestataires informatiques pour s'assurer de circonscrire le périmètre de l'attaque et interrompt toutes activités autres que la diffusion en attendant que la sécurité soit rétablie. Elle refuse de payer la rançon et mais aucune donnée supplémentaire n'est diffusée.

Les entreprises partenaires de la chaîne de médias qui ont été lésées (coproducteurs de contenus) demandent réparation des préjudices liés à l'anticipation de résultats moindres sur les productions dont les scénarios sont publiés. L'attaque s'étant ébruitée auprès de nombreux annonceurs, la chaîne voit ses recettes diminuées du fait de la baisse de ses rentrées publicitaires. L'entreprise consent également d'importantes dépenses pour le maintien de son image auprès de son audience, ce qu'elle parvient à faire puisque les consommateurs n'ont pas été touchés directement.

Viennent s'ajouter à ces pertes des pénalités contractuelles liées à la perte de confidentialité des contrats publicitaires, qui sont pour partie non-assurables. Les pertes majeures sont donc liées à la réparation de préjudices causés à des tiers ou au paiement de pénalités.

Scénario 6 : Banque

Une banque emploie une dizaine de milliers de salariés et dégage un résultat d'un demi-milliard d'euros. L'essentiel de son activité réside dans le crédit et le placement et est complétée par quelques services annexes. Une bonne partie de ses moyens humains est dédiée à l'accueil et au conseil dans les agences physiques. L'entreprise dépend fortement de son système d'information pour tracer l'ensemble des transactions qu'elle effectue et maintenir les données de sa clientèle.

Un intrus dans le système d'information parvient à effectuer un nombre important de transactions de faibles montants entre les comptes courants des clients de la banque et des comptes qui lui permettent de récupérer les fonds. L'attaque n'est détectée qu'après quelques jours. Des experts informatiques parviennent à s'assurer de la fin de l'attaque après que plusieurs milliers de comptes ont été touchés pour un montant cumulé d'un million d'euros. Un travail important est mené pour identifier les transactions illicites dont seule une faible proportion peut être annulée.

La banque doit notifier l'ensemble des clients touchés par les transactions frauduleuses que la banque entreprend spontanément de dédommager à hauteur des montants dérobés. Elle mène également une campagne importante de communication afin d'endiguer le départ des clients dont une partie des données personnelles, y compris la situation financière, a pu être diffusée. Toutefois, la perte de confiance dans l'institution provoque le départ de près de 10% de la clientèle, occasionnant des pertes d'exploitation considérables ainsi que des frais de réorganisation, dont des fermetures d'agences.

Les pertes financières directes et pour les clients ne représentent donc qu'un montant limité par comparaison avec les pertes indirectes occasionnées par la diminution de l'activité. Des frais exceptionnels (communication, notification et gestion de crise) sont également considérables. Une amende administrative pour manque manifeste de sécurisation du système d'information dans une activité manipulant des données à caractère personnel vient ajouter 20 millions d'euros de pertes non-assurables.

Un besoin d'analyse adapté à chaque entreprise

Des scénarios précédents se dégage évidemment l'impression d'une grande variété. Sans prétendre à l'exhaustivité, voici quelques éléments qu'il semble utile de noter. Tout d'abord, la nature des pertes occasionnées par des sinistres d'origine cyber dépend sensiblement de la configuration de l'entreprise visée : ses clients, ses fournisseurs, son niveau de dépendance à son système d'information. Cette configuration détermine également la capacité de l'entreprise à faire face à un sinistre.

Sans permettre des analyses très systématiques, notamment sur le niveau potentiel de pertes, le secteur d'activité et la taille d'une entreprise semblent être deux données importantes dans l'identification des menaces majeures et actifs ou processus critiques. La taille est également un indicateur de la capacité de l'entreprise à gérer par elle-même les conséquences d'un sinistre.

Certes, quelques pertes ne sont pas assurables : amendes, pénalités contractuelles notamment. En cela, rien ne change vraiment avec le risque cyber, mais la nouveauté qu'il nous semble utile de retenir est que l'ensemble des lignes de produits d'assurance est susceptible de se placer en soutien de la résilience des entreprises dans un contexte de forte numérisation. De l'expertise et l'analyse de l'assureur découlera la mobilisation des briques assurantielles adaptées au profil de l'assuré.

		Scénario 1 : PME de vente en ligne	Scénario 2 : PME de services informatiques	Scénario 3 : Entreprise de la grande distribution	Scénario 4 : Port de marchandises	Scénario 5 : Entreprise de médias	Scénario 6 : Banque
Dommages de l'assuré	Dommages matériels	Moins de 1%		Plus de 10%	Moins de 1%		
	Pertes financières directes						Moins de 1%
	Pertes d'exploitation	Plus de 10%	Moins de 1%	Entre 1% et 10%	Entre 1% et 10%		Plus de 10%
	Frais supplémentaires de gestion de crise	Entre 1% et 10%	Moins de 1%	Entre 1% et 10%	Moins de 1%	Moins de 1%	Moins de 1%
	Frais consécutifs à une violation de confidentialité						Entre 1% et 10%
	Frais liés à la sauvegarde de la réputation		Moins de 1%			Entre 1% et 10%	Moins de 1%
	Protection juridique	Moins de 1%	Entre 1% et 10%		Moins de 1%	Entre 1% et 10%	Moins de 1%
Dommages causés à des tiers	Dommages matériels aux tiers			Entre 1% et 10%	Plus de 10%		
	Dommages immatériels consécutifs				Entre 1% et 10%		
	Dommages immatériels non-consécutifs		Plus de 10%	Entre 1% et 10%		Plus de 10%	Moins de 1%
	Dommages corporels				Moins de 1%		
	Frais de retrait - dépose - repose		Moins de 1%				
	Défense recours	Entre 1% et 10%	Entre 1% et 10%	Entre 1% et 10%	Entre 1% et 10%		Entre 1% et 10%
	Responsabilité des mandataires sociaux		Entre 1% et 10%	Entre 1% et 10%	Moins de 1%	Moins de 1%	Moins de 1%
Pertes non-assurables	Pénalités de retards				Entre 1% et 10%		
	Autres pénalités contractuelles		Moins de 1%			Plus de 10%	
	Amendes administratives						Entre 1% et 10%

Ordre de grandeur de la perte en part du résultat net	Moins de 1%	Entre 1% et 10%	Plus de 10%

Tableau 2 : Impacts comparés sur des entreprises variées de sinistres d'origine cyber.

IV. Des entreprises aux besoins variés

Les risques cyber représentent une modification transversale des profils de risques des entreprises à laquelle on ne peut répondre de manière générique et universelle. Une classification par secteurs d'activité et par taille des entreprises constitue une première grille de lecture adaptée pour la sensibilisation aux leviers d'action.

Avant de parler d'assurance, ces leviers doivent se concentrer sur la mise en place d'une gouvernance du risque de niveau exécutif, contenant des composantes organisationnelle et budgétaire et brisant les silos entre les directions des systèmes d'information, de gestion des risques et des assurances ou encore des métiers. De cette gouvernance émergera la définition des scénarios critiques pour l'entreprise et les arbitrages sur leur traitement : prévention pour en réduire la fréquence et les conséquences estimées, risque résiduel assumé ou transféré à un marché d'assurance.

L'assurance n'est pas caduque face aux risques cyber car la plupart des scénarios ont des conséquences connues et habituellement couvertes. L'ensemble des polices d'assurance pouvant être déclenchées par un fait générateur cyber, la réflexion doit être plus globale que les offres dites « cyber » : elles ont un intérêt pour certains scénarios mais ne peuvent prétendre couvrir l'ensemble des risques. L'inclusion de services de gestion crise est en revanche une nouvelle garantie centrale pour la réaction à tout sinistre numérique et mérite d'être proposée dans toutes les polices couvrant des scénarios cyber.

Enfin, la numérisation n'a pas rendu assurables le risque d'entreprise ou les risques illicites : le vol de propriété intellectuelle, la chute de cours de bourse, la perte de réputation, la perte de marchés futurs, les rançons, les amendes ou encore les pénalités contractuelles ne relèvent pas de l'assurance. Recentrons les débats sur les questions prioritaires de gouvernance du risque et de révision des polices souscrites.

À chaque entreprise son profil de risque

Le remède universel aux risques cyber n'existe pas car les entreprises sont toutes soumises à un profil de risque particulier. Les scénarios décrits précédemment illustrent que l'analyse de risques ne peut se faire indépendamment de l'entreprise que l'on considère.

Une même typologie de sinistre ne va pas avoir les mêmes implications sur la capacité d'une entreprise à remplir sa tâche. L'indisponibilité du site internet d'une

entreprise ne concerne que quelques techniciens du SI en règle générale mais représente une crise majeure dans le cas d'une entreprise de vente en ligne. Le risque de vol de données personnelles fait frémir le maillon final des chaînechaînes de valeur vendant directement aux consommateurs mais est souvent négligeable en comparaison de la valeur des actifs à protéger des grands industriels.

La menace pesant sur chaque entreprise est à analyser en fonction de son envergure stratégique. Toutes les entreprises doivent se prémunir des escroqueries balayant un spectre large de cibles étant simplement connectées à internet mais certaines doivent également envisager des attaques plus ciblées à des fins d'espionnage ou de sabotage. La taille de l'entreprise et de ses concurrents, l'importance du secret manipulé ou encore la place systémique d'une entreprise au sein d'un état influencent l'ampleur de cette menace. La menace à prendre en compte n'est bien entendu pas limitée aux tiers extérieurs à l'entreprise : les collaborateurs représentent un vecteur de risque important, qu'il s'agisse de malveillance ou d'erreur.

La réponse pour traiter un risque particulier dépend également de l'entreprise considérée. Pour chaque scénario, un équilibre doit être trouvé entre de l'investissement préventif et un transfert vers le marché d'assurance : cela définit l'appétit au risque. Prenons le cas d'un producteur d'électricité : la fourniture de son service en tout temps est l'essence de son activité et son appétit au risque d'interruption de la production est par nature très faible. La protection de données personnelles est en revanche plus éloignée de son cœur de métier et ses investissements dans ce domaine pourraient se limiter à une conformité à la réglementation. Le risque résiduel assumé serait alors d'un ordre de grandeur supérieur à l'interruption de service et le transfert vers l'assurance plus important.

Retenons tout de même que ces deux composantes de traitement du risque ne sont pas parfaitement substituables. Disposer d'une assurance ne réduit pas nécessairement l'effort de prévention car les conséquences de la perte de confiance des acteurs économiques engendrée par un sinistre peuvent être bien supérieures à la couverture assurantielle, qui n'a jamais prétendu annuler les risques pesant sur l'entreprise. La taille de l'entreprise est également déterminante dans le traitement du risque : là où une grande entreprise a la force de frappe suffisante pour la mise en place des organes de gouvernance, des processus de management du risque et des compétences techniques de prévention et de gestion de crise, une petite entreprise devra se reposer sur un écosystème de prestataires remplissant ces fonctions.

Cette variété de profils de risques nous convainc aisément qu'une réponse unique ne suffira pas, qu'elle soit assurantielle ou non. Pour orienter la réflexion, nous

recommandons de mettre en avant une grille d'analyse basée sur la taille de l'entreprise et son secteur d'activité. C'est une première approche qui n'englobe pas totalement la spécificité nécessaire au traitement du risque dans chaque entreprise mais qui permet déjà d'y voir plus clair et d'être effectif dans la transmission du savoir. Les fédérations professionnelles nous paraissent être un levier efficace pour cette mission : en capitalisant sur l'expérience acquise par les entreprises les plus matures dans un secteur, elles peuvent mener les réflexions et fournir des recommandations adaptées à l'activité pour la cartographie des risques, son évolution, et son traitement.

Une réponse transversale aux risques de la révolution numérique

Pour optimiser son action, l'entreprise se transforme en se reposant toujours plus sur des outils numériques. En contrepartie, elle se rend dépendante de leur fonctionnement, elle devient « cyberdépendante ». Cette dépendance dépasse le cadre de la gestion des systèmes d'information traditionnelle, elle est transversale au sein de l'entreprise.

Le département informatique et en particulier le responsable de la sécurité des systèmes d'information est habitué à gérer un risque informatique technique : protection contre les virus, disponibilité des machines et des données. En cas de sinistre, il utilise un plan de continuité d'activité ou de reprise d'activité qu'il a élaboré. Le département de gestion des risques et des assurances a en charge la cartographie des risques métiers et financiers. Les acteurs du métier comprennent les implications des usages numériques sur leur travail quotidien. Les départements de conformité et d'audit sont garants de la mise en place des procédures préventives. Le comité exécutif arbitre le budget entre les directions et définit son appétit aux risques. Enfin, tous les collaborateurs sont des vecteurs potentiels d'attaque cyber dans leur usage du système d'information. Pour traiter le risque cyber, c'est donc l'ensemble de ces acteurs qu'il est nécessaire de faire communiquer autour d'un même objectif. La transversalité de ce problème impose la mise en place d'une gouvernance de haut niveau.

Nous avons rencontré des entreprises de divers niveaux de maturité dans le traitement du risque cyber. Trop souvent un travail en silo empêchant un traitement transversal est décrit, la direction des systèmes d'information ayant peu de contacts avec celle des risques et des assurances par exemple. Trop souvent la question de l'assurance contre un risque cyber générique est envisagée sans étude profonde de l'impact du numérique sur la cartographie des risques. Trop souvent les instances de

direction ont pris conscience de la matérialité du risque sans parvenir à la mise en place d'une gouvernance organisée et de budgets dédiés[8].

De l'autre côté du spectre, plusieurs entreprises sont matures et motrices sur le sujet. Certaines ont un membre du comité exécutif dédié à la gestion du risque, qu'il ait le titre de *chief (digital) risk officer* ou qu'il soit responsable de la transformation numérique. D'autres ont un comité des risques mettant régulièrement autour de la table l'ensemble des acteurs concernés. Toutes ont une réflexion de niveau exécutif, avec un arbitrage avisé sur l'acceptabilité et l'appétit au risque, le transfert possible d'un risque résiduel au marché d'assurance ou sa gestion interne dans une captive. En exemple de traitement du risque cyber, nous tenons à noter la démarche mise en place par Airbus Defence and Space en 2015, nommée méthode SPICE[9], qui vise à identifier et estimer les conséquences financières des risques numériques dominants à l'échelle du groupe, en recueillant l'expertise des opérationnels.

Nous ne saurions préconiser un mode de gouvernance particulier qui dépend fortement de l'organisation et du type d'entreprise et pour lequel plusieurs recommandations existent par ailleurs [8] [9] mais nous nous concentrons sur les quelques points qui nous semblent déterminants dans le traitement du risque :

- l'assurance n'est qu'un moyen de transfert de risque résiduel et ne saurait se substituer ou être souscrite en amont d'une réflexion plus globale. En particulier, l'appétit au risque et le caractère transférable ou non des risques sont des choix avisés,
- la numérisation transforme l'ensemble des risques de l'entreprise et doit se traiter transversalement, avec une organisation et des budgets dédiés, décidés par les plus hautes instances,
- l'utilisation de scénarios réalistes permet de parler concrètement des risques et d'estimer leurs impacts,
- l'activité, les risques et leur matérialité évoluent, donc la réflexion doit être régulière.

---

[8] Voir le rapport de McAfee décrivant même une différence de perception sur le niveau de maturité de traitement du risque entre les dirigeants et les collaborateurs [16]

[9] Scenario Planning for Identification of Cyber Exposure. Voir le rapport du séminaire de recherche de l'IRT SystemX [17] pour plus de détails.

Quelques leviers nous paraissent intéressants pour inciter les entreprises à mettre en place cette gouvernance. L'information financière annuelle pourrait être enrichie sur le sujet en décrivant plus précisément la gouvernance et les actions mises en place pour traiter les risques liés à la transformation numérique. Un administrateur pourrait également être identifié pour être responsable devant les actionnaires de la bonne gouvernance du risque par les dirigeants.

L'assurance n'est pas caduque face aux risques cyber !

A présent que l'accent a été mis sur un traitement transversal du risque dans l'entreprise, nous pouvons nous autoriser à parler d'assurance, dernier maillon de la chaîne de gestion des risques. C'est à partir de la démarche de gouvernance mise en place par l'entreprise qu'émerge l'expression de besoins de transfert d'un risque résiduel vers l'assurance.

Nos scénarios illustratifs montrent que le risque cyber ne peut se traiter à l'aide d'une solution unique, une « assurance des risques cyber » : il ne s'agit pas d'une nouvelle catégorie autonome de risques mais d'une modification globale du profil de risques. Pour autant, cela ne signifie pas que l'assurance est caduque : la plupart des conséquences des sinistres cyber sont des phénomènes connus de l'assurance et couverts dans des polices usuellement souscrites par les entreprises.

Plus fortement encore, nous voulons souligner que l'ensemble des polices d'assurance souscrites par l'entreprise peut entrer en jeu dans le cas d'un sinistre cyber dimensionnant. En reprenant les plus grandes catégories de préjudices couverts par l'assurance, les attaques cyber décrites ont engendré :

- des dommages matériels aux biens de l'entreprise dans le cas de la perturbation des données de stocks du distributeur,
- des dommages matériels à des biens appartenant à des tiers à l'entreprise dans le cas de la prise de contrôle des grues du port de marchandises,
- des dommages immatériels à l'entreprise sous forme de pertes d'exploitation dans le cas de l'attaque en déni de service sur le site internet de la PME de vente en ligne,
- des dommages immatériels à des tiers sous forme de pertes financières sèches aux clients de la banque dans le cas des transactions financières frauduleuses.

Le besoin de transfert du risque résiduel vers l'assurance se détermine donc lors d'une réflexion globale, en confrontant l'ensemble des polices souscrites aux scénarios critiques, afin de les adapter aux modifications du profil de risque. Quant

aux polices dites « cyber » aujourd'hui, elles apportent quelques couvertures nouvelles qu'il s'agit de souscrire lorsqu'elles sont pertinentes dans le scénario, comme celui du vol de données chez l'entreprise de médias : couverture de l'immatériel non-consécutif à un dommage matériel comme la perte d'exploitation et les frais supplémentaires ou encore fourniture de services de gestion de crise permettant de minimiser le préjudice financier et réputationnel.

Mais l'assurance n'est pas la panacée

La réflexion des entreprises sur leurs risques liés à la transformation numérique les amène à identifier des préjudices potentiels de taille critique non couverts par l'assurance. Elles sont alors tentées de transférer ces risques : la chimère de l'assurabilité du risque d'entreprise est remise sur le devant de la scène.

La numérisation rend les attaques sur le capital informationnel des entreprises plus faciles, moins coûteuses et indépendantes de toute contrainte géographique. L'intelligence ou la guerre économiques font planer des risques sur la réputation, la propriété intellectuelle, les marchés futurs, la clientèle, les opportunités, les avantages compétitifs ou encore le cours de bourse. Malheureusement, même dans un contexte de numérisation massive, ces risques ne relèvent pas de l'assurance : le préjudice étant non certain et d'une valeur non estimable, ils contreviennent directement au principe indemnitaire. Toute tentative d'indemnisation, même basée sur un système complexe de calcul paramétré, pourrait mener à l'enrichissement de l'entreprise par rapport à sa situation précédant le sinistre et relève ainsi plus de la spéculation que de l'assurance.

Illustrons ceci par un exemple : une jeune entreprise développe depuis plusieurs mois et en secret un jeu vidéo, qui sera son produit phare pour l'année à venir. Sur les marchés visés, elle est en concurrence avec des firmes mieux installées, moins innovantes sur le plan artistique mais parvenant à développer leurs produits beaucoup plus rapidement. L'une d'entre elles s'introduit dans le SI de l'entreprise initiale, s'empare du scénario et de quelques croquis et, sur cette base, commercialise un jeu avant la première. Ce sont des mois de développement gâchés, et la perte certaine d'un marché jugé prometteur. Après un recours sans suite et désertée par ses investisseurs, l'entreprise dépose le bilan en quelques mois. On pourrait chercher à indemniser la perte de marché futur subie au titre du vol de propriété intellectuelle, qui resterait par ailleurs à établir, mais il est manifeste que cela ne conduirait qu'à enrichir les apporteurs initiaux et ne permettrait en aucun cas à l'entreprise de poursuivre ses activités. De plus, comment chiffrer le préjudice en l'absence d'une

base de comparaison qui correspondrait au scénario dans lequel la première entreprise aurait eu la primeur de la commercialisation de son produit ?

En réalité, ce type de scénario n'est pas une nouveauté liée à la numérisation. Lorsqu'un centre de recherche et développement prend feu et qu'une entreprise perd une partie de la propriété intellectuelle qui aurait pu lui permettre de conquérir un nouveau marché, l'assureur n'est pas en mesure de l'indemniser au titre de la perte de ce marché potentiel. Ainsi, la donnée en tant que telle n'est pas devenue assurable parce qu'elle a été numérisée et le risque d'entreprise reste encore à la charge des entreprises.

D'autres types de risques financiers monopolisent les débats sur l'assurabilité. Les amendes reviennent tout d'abord dans la lumière avec l'entrée en vigueur prochaine du Règlement Européen pour la Protection des Données Personnelles qui introduira des amendes administratives de taille conséquente aux contrevenants d'un défaut de traitement des données personnelles (jusqu'à 4% du chiffre d'affaire mondial ou 20M€). De même que les amendes pénales, les amendes administratives ne sont pas assurables car elles ne correspondent ni à un risque licite ni à un risque involontaire. Ensuite, les *ransomwares* étant devenus le type d'attaque cyber le plus médiatisé[10], l'assurabilité des rançons est remise en question. La réglementation française prévenant toute action conduisant au financement du terrorisme[11], il n'est pas légalement envisageable de couvrir le paiement d'une rançon par de l'assurance. Enfin, le paiement de pénalités contractuelles pose question : bien que ne relevant pas de l'illégalité, l'assurance de telles pénalités les viderait de leur substance punitive et ne favoriserait pas leur bon dimensionnement. Si certains assureurs peu scrupuleux usent aujourd'hui de ces garanties comme produit d'appel tout en rétablissant leur conformité au droit via un astérisque mentionnant « seulement là où la loi le permet », c'est que le droit mérite d'être réaffirmé et les pratiques de distorsion de concurrence éventuelles encadrées. En revanche, cela ne nécessite pas de débats plus approfondis sur l'assurabilité de ces risques.

L'ensemble de ces débats tend à détourner l'attention des besoins réels des entreprises en pleine transformation numérique. L'assurance a pourtant un rôle déterminant à jouer dans leur accompagnement, à condition qu'elles en tirent parti correctement.

---

[10] Première cause de sinistres cyber déclarés à AIG EMEA entre 2013 et 2016 [15].

[11] Article 421-2-2 du code pénal

V. Le rôle de l'assureur dans la révolution numérique

Afin d'adapter sa couverture aux profils de risque en évolution des entreprises, l'assurance doit instaurer un dialogue avec ses clients permettant de comprendre leur besoin et d'y apporter la solution assurantielle la mieux adaptée. Une telle solution devrait s'appuyer sur des scénarios qui apportent une compréhension concrète et personnalisée des risques critiques, elle devrait couvrir positivement et explicitement les risques identifiés en évitant autant que possible l'ambiguïté et les couvertures « par défaut » et enfin elle devrait indemniser les conséquences d'un sinistre à la même hauteur quelle que soit son origine a priori.

Les spécificités du cyber entraînent une forte dépendance des profils d'exposition à la taille et au secteur d'activité de l'entreprise : l'assureur devrait en tenir compte pour définir une offre la plus adaptée possible. Il pourrait également se placer en fournisseur des services jugés nécessaires à la gestion des risques cyber : conseil en gestion et mitigation du risque, gestion de crise et remédiation. Il devrait en tout cas s'abstenir d'imposer une solution universelle promettant une couverture exhaustive des risques cyber, comme le marché actuel semble le proposer.

Le pragmatisme des scénarios au service d'un dialogue constructif

Dans le cadre de leur *risk management*, les entreprises identifient des scénarios dimensionnants menaçant leurs processus critiques. Une gouvernance efficace du risque consiste alors à se prémunir contre ces menaces identifiées et à les mitiger pour ensuite être en mesure d'arbitrer entre les risques résiduels dont l'impact peut être absorbé en interne et ceux, potentiellement trop intensifs en capitaux, que l'entreprise préfèrera transférer à l'assurance. L'enjeu pour elle est crucial car il s'agit de garantir sa continuité d'activité sur le plan opérationnel mais également le maintien de sa légitimité à mener sa raison sociale.

L'assureur joue donc un rôle clé dans cette chaîne de valeur en apportant les briques assurantielles permettant de couvrir les processus critiques de l'entreprise et de garantir sa résilience en absorbant les conséquences financières d'un sinistre. Or la transformation numérique a introduit une dépendance forte des entreprises à leur système d'information dont la disponibilité, la confidentialité et l'intégrité est devenue nécessaire à leur activité. De nouveaux scénarios sont apparus et il semble crucial pour l'assureur de ne pas les ignorer s'il souhaite continuer à jouer son rôle historique et à offrir une protection efficace de la résilience des entreprises.

Afin de prendre en compte de manière pertinente l'impact du cyber sur les profils de risque des entreprises, il nous paraît nécessaire de souligner l'importance pour l'assureur de se baser sur les scénarios que l'entreprise a identifiés pour mieux comprendre le risque auquel elle est exposée. Face à une menace cyber nouvelle, dématérialisée et difficile à définir, une telle méthode offre l'avantage de mettre en évidence de manière concrète les risques qui pèsent sur l'entreprise en partant des conséquences opérationnelles que les équipes métiers identifient comme critiques. Elle apporte donc une clarté et un pragmatisme qui seront utiles à l'assuré mais également à l'assureur dans le cadre de sa démarche de construction d'une couverture adaptée au besoin de son client ainsi qu'à son besoin propre de rentabilité et de gestion des cumuls.

L'utilisation de scénarios permet tout d'abord à l'assureur d'évaluer l'ampleur maximale des sinistres auxquels est exposé son client. C'est particulièrement vrai dans le cadre industriel où les scénarios critiques portent principalement sur l'intégrité et la disponibilité d'actifs physiques (machines, infrastructures, etc) qui étaient déjà couverts avant la révolution numérique et dont l'assureur sait en estimer le coût. En effet, contrairement au fantasme très répandu d'une menace cyber bouleversant les problématiques de sécurité des entreprises, celle-ci se contente bien souvent d'exacerber des risques critiques qui existaient déjà, en en faisant varier éventuellement la surface d'attaque. Par exemple, les problématiques de confidentialité des données personnelles introduites par le cyber ne constitueront somme toute qu'un enjeu négligeable pour une entreprise pétrolière en comparaison de son risque existant d'explosion de raffinerie que l'assurance est déjà en mesure de couvrir.

Les scénarios sont également un moyen pour l'assureur de mesurer la fréquence d'occurrence de certains sinistres. En mettant à profit son historique actuariel et la connaissance tirée de la transversalité de ses clients il peut identifier, dans chaque scénario, les causes les plus probables et en estimer la probabilité d'occurrence. La « probabilité d'une attaque cyber » paraît impossible à calculer, en revanche si un client met en évidence que seuls les scénarios reposant sur l'indisponibilité d'un certain serveur sont critiques alors il devient facile d'en prévoir la sinistralité moyenne en en considérant les causes les plus probables (*DDoS*, *ransomware*, prise de contrôle, etc) et les probabilités d'occurrence.

Les scénarios permettent enfin et surtout de centrer la conversation sur les problématiques propres à chaque assuré et d'éviter ainsi les débats stériles, par exemple sur la nécessité ou non de couvrir des ordinateurs déconnectés du système

de production ou de caméras de surveillance réglementaires inoffensives. En ce sens ils permettent une approche rationnelle d'un risque mal compris et doivent donc selon nous constituer la base du dialogue entre l'assureur et l'assuré.

Lever une ambiguïté préjudiciable à toutes les parties

Il règne actuellement une ambiguïté sur l'état des couvertures assurantielles cyber souscrites. Le manque de lisibilité de l'offre assurantielle en ce qui concerne le cyber génère une incertitude que beaucoup d'entreprises choisissent de ne pas voir. En effet, même si cela n'est pas la norme, certaines d'entre elles complètent leurs couvertures spécifiques par des polices « tous risques sauf » – c'est-à-dire couvrant tout type de sinistre dans un certain cadre à l'exception de cas particuliers qu'il convient à l'assureur d'indiquer explicitement dans le contrat. Cette démarche leur permet de se prémunir contre des risques qui auraient pu échapper à leur analyse interne ou, dans le cas des plus petites, parce qu'elles ne sont pas en mesure d'effectuer un telle analyse de risques. Ces polices déjà souscrites par les entreprises devraient donc juridiquement couvrir les conséquences d'une attaque cyber dès que celles-ci ne sont pas explicitement exclues ce qui laisse penser que le cyber serait alors couvert par défaut. Il s'agit d'une « couverture silencieuse » ou « *silent cover* » qui peut être activée pour des sinistres que l'assureur n'avait pas anticipés au moment de la rédaction du contrat et qui peut toujours échapper à sa conscience. Ainsi certaines entreprises, partant du principe simplificateur que l'ambiguïté leur sera favorable, s'estiment correctement protégées et refusent de se pencher sur cette problématique ou de mettre à jour leur couverture afin de prendre correctement en compte l'impact du cyber sur leur besoin assurantiel.

Assureurs : sortir de la zone grise

Les assureurs de leur côté, peuvent avoir une image erronée de leur solvabilité car ils ne sont pas encore en mesure de percevoir directement l'impact du cyber sur leurs portefeuille de polices pour plusieurs raisons :

- Tout d'abord, même en incluant les nouveaux risques d'origine cyber, la numérisation engendre en général plutôt une baisse qu'une hausse de la sinistralité, du fait de procédés optimisés et mieux contrôlés. Une machine connectée sera certes vulnérable au piratage mais en contrepartie elle pourra vérifier sa configuration, optimiser sa charge de travail, planifier son entretien et sera donc beaucoup moins susceptible de tomber en panne ou d'être brisée suite à une erreur de manipulation qu'une machine similaire actionnée par un être humain.

- Ensuite, la nature cyber de l'origine d'un sinistre, en particulier quand il n'est pas directement lié au système d'information, est souvent très difficile à détecter et à établir. Les intrusions informatiques peuvent laisser suffisamment peu de traces pour ressembler à de simples défaillances informatiques, relativement courantes et aux conséquences similaires.
- De plus, par souci de préservation de leur image ou simplement par ignorance de l'existence d'une couverture associée dans leur contrat, les entreprises décident parfois de ne pas déclarer de tels sinistres, préférant en traiter les conséquences en interne.
- Enfin les conséquences d'une attaque cyber sont souvent difficilement chiffrables et constituent surtout une gêne à l'activité (écran ou matériel informatique hors service, emails inaccessibles pendant quelques heures, etc) qui sera rattrapée au sein de l'entreprise sans que ne soit fait l'effort d'essayer de leur attribuer un coût. Dans ces cas-là non plus, aucun dossier ne sera envoyé à l'assureur.

Le peu de demandes d'indemnisation suite à un sinistre identifié clairement comme d'origine cyber masque probablement l'exposition réelle que prennent les assureurs sur les risques cyber et les pousse à ne pas en tenir compte. Lorsqu'ils sont effectivement pris en compte, il sont plus souvent exclus ou restreints à l'aide de sous-limites que pleinement traités.

Cette complaisance de part et d'autre dans le refus de considérer le problème n'est évidemment pas favorable au développement d'un marché sain et équilibré. Cette ambiguïté commence cependant à faire surface chez les réassureurs qui s'inquiètent d'un *silent coverage* peut-être trop généralisé dans les polices de leurs clients et qui pourrait leur faire porter un risque systémique qu'ils ne sont pas sûrs de pouvoir mutualiser efficacement. Il est très clair que ce flou ne profite finalement à aucune des deux parties.

Une ambiguïté qui profite à l'assuré ?

Pour l'assuré, ignorer cette ambiguïté revient à repousser son traitement au moment de la survenance d'un sinistre. Alors que l'entreprise sera prise à parti par la gestion critique de sa crise, elle devra en parallèle identifier quelles conséquences sont susceptibles d'être indemnisables, laquelle ou lesquelles de ses polices peuvent jouer, vérifier que l'origine du sinistre survenu n'en est pas exclue, le tout en négociation tendue avec l'assureur voire les différents assureurs concernés. Etant donné la confusion que cela engendre, même dans le cas où le sinistré arriverait à obtenir l'indemnisation de son sinistre, il y a fort à parier que cela se fera avec des semaines

voire des mois de retard et qu'il devra de plus accepter par la suite l'ajout d'une exclusion cyber sur son contrat. Avec le resserrement des échelles de temps autour d'un sinistre cyber, il semble donc particulièrement utile à l'assuré d'avoir anticipé ce risque et identifié en avance les polices à faire jouer en collaboration avec l'assurance.

Cela lui permettra dans un premier temps de détecter les éventuels « trous de couverture », ces nouveaux risques introduits par le cyber (confidentialité des données, dommages immatériels non-consécutifs en responsabilité, etc) et absents des polices traditionnelles et pour lesquels il conviendra le cas échéant de souscrire de nouveaux contrats spécifiques. Cela pourra aussi parfois mettre en évidence la présence de doublons de couvertures coûteux, inutiles et potentiellement générateurs de confusion à la survenance du sinistre si les assureurs concernés n'arrivent pas à s'entendre sur l'ordre de l'indemnisation. Sur le plan opérationnel, au-delà de la nécessaire gouvernance du risque en amont, la bonne gestion de crise est cruciale dans le cadre d'attaques cyber et détermine en grande partie le dimensionnement final du sinistre.

Il est donc primordial que les entreprises aient réfléchi au sujet, mis au point des cellules de crise, des plans de continuité d'activité et si elles sont techniquement incapables de traiter ce type de sinistre en interne qu'elles aient identifié les prestataires adaptés à la remédiation du sinistre. Ces démarches et frais supplémentaires doivent être déterminés à l'avance en lien avec l'assurance qui les couvrira et voudra des garanties sur leur efficacité à contenir et réparer rapidement les sinistres. S'il en est tenu au courant, l'assureur pourra également participer à la démarche de l'entreprise. Il sera en mesure de proposer une certaine expertise sur le sujet qu'il tire d'une compréhension statistique du risque permise par la taille de sa clientèle soumise à des risques similaires ainsi que par ses éventuels partenariats avec des prestataires techniques. De manière générale, persister à croire que l'ambiguïté lui profite n'incitera jamais l'entreprise à développer une bonne hygiène de compréhension du risque sur la base de scénarios.

Un risque de nature systémique

Pour l'assureur la problématique principale est celle de la gestion des cumuls potentiellement engendrés par une couverture silencieuse trop généralisée de risques d'origine cyber. En effet, la menace cyber est par nature extrêmement rapide et peut se propager à très grande échelle en exploitant l'interconnexion standardisée et peu sécurisée des acteurs. Elle revêt donc un caractère éminemment systémique et il y a un risque pour l'assureur qu'une très grande partie de ses assurés soient affectés par

une même attaque cyber à grande échelle et déclenchent leurs polices silencieuses simultanément, générant un besoin d'indemnisation trop important pour que l'assureur soit en mesure d'y répondre. Un tel scénario reste à venir mais les experts mettent en garde sur la forte probabilité de sa survenance dans les prochaines années. Il pourrait consister en un virus exploitant une faille non corrigée d'un système d'exploitation et capable de s'installer instantanément sur un très grand nombre de machines, dérobant leurs données et les paralysant, entraînant des dégâts immatériels et pertes d'exploitation à un très grand nombre d'acteurs.

On peut également penser au scénario de la grosse entreprise de service en ligne qui se retrouve incapable de fournir son service, par exemple suite à une attaque en déni de service, et qui fait subir simultanément à ses très nombreux clients des pertes substantielles du fait de leur incapacité à utiliser correctement les équipements ou procédés qui dépendaient de ce service. Dans tous les cas, de tels scénarios aux conséquences si graves ne sont pas encore survenus et il est impossible d'évaluer dans l'état actuel des choses leur probabilité d'occurrence. La solution pourrait venir des réassureurs que cette situation inquièterait et qui appelleraient leurs clients à effectuer la démarche d'évaluation de leur exposition cyber et des risques de cumul associés.

Il apparaît donc clairement que la couverture assurantielle d'un risque doit être explicite et que l'ambiguïté qui règne actuellement au sujet du risque cyber ne profite ni aux assurés, qui ne sont pas incités à le gérer convenablement et se retrouvent dans l'incertitude et la confusion engendrant une grande inefficacité au moment pourtant crucial de survenance du sinistre, ni aux assureurs qui sont exposés à leur insu à un risque potentiellement systémique. La purge de cette situation se fera par le dialogue entre l'assureur, ou éventuellement le courtier qui fera valoir son rôle de conseil, et l'assuré. Le régulateur des assureurs, l'ACPR, peut également avoir un rôle à jouer en imposant à l'assureur de connaître son exposition au risque cyber et en le forçant donc à clarifier ses contrats en ouvrant le dialogue avec ses clients.

Sans complètement exclure le cyber de leurs contrats traditionnels, certains assureurs y imposent toutefois des sous-limites dépendant de l'origine du sinistre. Par exemple un risque que l'entreprise aura estimé critique et jugé propice à un transfert à l'assurance sera bien couvert à la hauteur nécessaire mais avec une condition précisant que l'indemnisation n'excédera pas un certain montant, la sous-limite, dans l'éventualité où le sinistre surviendrait à la suite d'une attaque cyber. Ces conditions, qui peuvent sembler inoffensives à l'entreprise n'étant pas toujours consciente de son exposition cyber, sont parfois imposées par des assureurs frileux à

l'idée de s'engager dans le domaine. Dans d'autres cas, l'assureur pourra même choisir d'exclure complètement les sinistres d'origines cyber de son contrat mais proposer en contrepartie un second contrat très semblable, une police « dédiée cyber », couvrant explicitement les mêmes sinistres mais uniquement quand ceux-ci sont d'origine cyber. Un tel contrat sera alors plafonné à un niveau beaucoup plus faible que la police traditionnelle, rendant ainsi la couverture caduque dans ce cas.

Il est compréhensible que les assureurs mettent en place des systèmes permettant de mieux gérer leur exposition au cyber en isolant son impact au sein des polices traditionnelles, cependant les pratiques observées actuellement consistent souvent à imposer une sous-limite de l'ordre du dixième de la garantie standard, vidant ainsi complètement la couverture de sa substance. Le besoin de l'entreprise reste d'être indemnisé à la hauteur du préjudice qu'elle a subi afin d'être remise en l'état dans lequel elle était avant le sinistre. Il n'y a aucune raison de penser *a priori* qu'un sinistre aura des conséquences moindres quand il est d'origine cyber et par conséquent il n'y a pas de raison pour que la couverture dépende de l'origine du sinistre. Ces situations sont particulièrement probantes dans le cas de l'assurance contre la destruction d'actifs industriels très coûteux couverts à hauteur de plusieurs milliards mais presque intégralement exposés en cas d'attaque cyber car les assureurs refusent de fournir des couvertures suffisantes. Cette situation nous paraît peu convaincante et constitue un échec de l'assurance dans sa mission de garantie de résilience de l'assuré.

De plus il est parfois très difficile d'établir la cause exacte d'un sinistre, en particulier quand les actifs concernés sont physiquement détruits. Si les circuits d'une machine sont brûlés il devient difficile de retracer le dysfonctionnement à l'origine de la destruction. Une dépendance des niveaux de couverture à la cause peut alors entraîner une grande confusion, ni l'assureur ni l'assuré n'étant certains du montant à rembourser.

Une couverture idéale n'a pas d'odeur

Idéalement l'assureur devrait dans la mesure du possible couvrir les conséquences d'un sinistre indépendamment de son origine. L'étude des causes potentielles d'un sinistre permet d'en estimer la probabilité d'occurrence et donc influera sur le montant de la prime mais le niveau de couverture doit rester le même pour garantir au client la protection dont il a besoin. Si l'assureur détecte une surexposition au cyber d'un des actifs qu'il couvre, sa réaction devrait être d'en référer au client, l'inciter à une meilleure protection, éventuellement d'ajuster les primes en conséquence voire en dernier recours de refuser simplement d'assurer cet actif. Un

tel comportement, s'il était généralisé parmi les assureurs obligerait les entreprises à prendre pleinement conscience de l'exposition de chacun de leurs actifs sous peine d'être incapables de les assurer, ce qui serait très sain : seul un risque maîtrisé et assumé devrait être assuré.

En résumé, l'assurance dont les entreprises ont besoin pour faire face à leur transformation numérique remplit les objectifs suivants :

- couvrir les risques portant sur les processus et actifs clés de l'entreprise déterminés sur la base de scénarios spécifiques définis par l'entreprise,
- couvrir uniquement des risques maîtrisés que l'entreprise aura consciemment choisi de transférer,
- couvrir explicitement les faits générateurs cyber : à chaque scénario une police clairement identifiée,
- offrir un niveau de couverture indépendant de l'origine du sinistre.

L'aide à la gestion de crise, un rôle nouveau pour l'assureur

Lors d'un sinistre cyber, les échelles de temps sont contractées. L'attaquant a planifié méticuleusement son attaque depuis plusieurs années, il a déjà réussi à s'introduire dans le système sans se faire remarquer via des procédés d'ingénierie sociale et espionné discrètement les failles de l'entreprise depuis des mois. Il sait où, quand et comment frapper pour faire très mal. Il passe à l'action au pire moment, en soirée ou le weekend quand les techniciens sont chez eux, indisponibles. Les effets de l'attaque sont immédiats, les serveurs « tombent », les sites internet sont indisponibles ou redirigés vers des clones frauduleux, des emails sont envoyés au nom de l'entreprise, l'accès à internet est coupé sur le site, les services sont inaccessibles : tout est soudain paralysé. Les remontées se font rapidement mais par tous les canaux disponibles dans une confusion terrible. Les utilisateurs, les techniciens, le personnel sur site, les prestataires, les clients, les médias, tout le monde tente de proposer son explication. Pendant ce temps le système d'information est progressivement infecté, des données sont chiffrées ou volées, etc. A ce moment clé du sinistre, la réaction de l'entreprise va être cruciale.

- L'entreprise A n'a jamais anticipé un tel scénario. Elle est complètement perdue et il n'y a pas grand-chose qu'elle puisse faire. Le responsable de sécurité des systèmes d'information (RSSI), seul sur site et dépassé par les évènements finira par débrancher l'intégralité du parc informatique, mettant un terme à l'attaque – et à l'activité propre de son entreprise – mais sans en réparer les conséquences. Une conférence de presse le lendemain tente

confusément de rassurer sans préciser si des données ont été perdues ni quand le service sera rétabli…

- L'entreprise B appelle rapidement ses prestataires de gestion de crise et de remédiation identifiés au préalable qui se rendent immédiatement sur place avec les techniciens et responsable du SI de l'entreprise. Via des outils de monitoring du réseau ils identifient quelles machines sont infectées et les déconnectent du réseau. Le site web est redirigé vers un serveur sain qui offre un service en mode dégradé et affiche un message d'explication et d'excuse aux utilisateurs. Pendant que les techniciens de l'entreprise rétablissent les bases de données à partir de la dernière sauvegarde, les prestataires étudient les historiques des machines infectées et retracent le schéma d'attaque permettant d'identifier la faille exploitée et d'appliquer le correctif de sécurité adapté aux nouvelles machines mises en service. Le comité exécutif autorise une communication transparente sur les réseaux sociaux qui informent en temps réel de la progression de la situation, laquelle est rapidement sous contrôle.

On le voit dans ces exemples fictifs : de la qualité de la gestion de la crise lors de sa survenance dépend fortement l'ampleur de l'impact final du sinistre. C'est notamment le cas sur les coûts liés à une atteinte à l'image, à une perte de réputation ainsi qu'aux frais légaux consécutifs à une attaque cyber. Un service de gestion de crise et de remédiation efficace et clairement identifié au préalable est donc un atout clé pour l'entreprise dans le cadre de sa gestion du sinistre. De la même façon que lorsqu'il couvre un incendie, l'assureur demande la mise en place de détecteurs de fumée, sprinklers et s'assure que les pompiers peuvent accéder rapidement au site, l'assureur qui choisira de porter les conséquences financières des sinistres cyber aura également un fort intérêt à vérifier que son client a bien effectué cette démarche d'identification des services destinés à circonscrire les crises cyber.

Un service encore plus utile dans les petites entreprises

Dans le cadre des plus petites entreprises, ces services pourront être recommandés par l'assureur voire directement inclus dans son offre. Ce nouveau marché peut constituer selon nous un levier de croissance pour l'assureur qui a ainsi l'opportunité de se placer sur un segment plus long et moins intensif en capital de la chaîne de valeur associée à la gestion du risque :

- L'assureur pourrait d'abord jouer le rôle de *risk manager* que l'entreprise n'est pas en mesure de développer en interne et proposer les scénarios

standardisés qu'elle constate comme généralement critiques chez sa clientèle de taille et secteur d'activité comparable.

- Il pourrait ensuite conseiller son client sur les méthodes de protection à mettre en place, sa légitimité provenant de l'expertise tirée de sa connaissance transversale du risque permise par la diversité de sa clientèle.
- Enfin, il jouerait le rôle d'intermédiaire entre l'entreprise et les prestataires de service de gestion de crise et de remédiation, garantissant la qualité de service de ce dernier. On notera que les prestataires de sécurité seront de leur côté peu enclins à intégrer une assurance à leur service, une telle démarche pouvant passer pour un aveu de la faiblesse de leur solution. L'assureur est donc bien le mieux placé pour développer ce partenariat.

La liberté de choix du prestataire devrait par ailleurs être garantie si l'entreprise assurée est en mesure d'identifier par elle-même le plus pertinent.

Pour les plus grandes entreprises, il est en revanche impensable que l'assureur devienne prescripteur de solutions de cyber sécurité. Celles-ci doivent être en mesure de gouverner leur propre risque en interne et souhaiteront contracter directement les solutions qui leur paraissent les mieux adaptées à leur besoin sans en référer à l'assureur, notamment du fait des sujets régaliens qui doivent naturellement être traités en interne. En effet, l'assureur ne peut pas prétendre recommander un prestataire de sécurité sans rentrer dans le détail des opérations de son client et compromettre donc la confidentialité de ses procédés. La solution assurantielle adaptée ne pourra émaner que de la définition de son besoin par l'entreprise.

Une offre « cyber » universelle inadaptée

Le dogme anglo-saxon consiste à exclure les conséquences des sinistres d'origine cyber des polices traditionnelles pour ensuite proposer de nouvelles polices cyber spécifiques présentées comme une nouvelle ligne de produit et une opportunité de croissance. Une telle offre a certes le mérite de clarifier et segmenter l'exposition cyber de l'assureur mais elle est source de complexité pour l'assuré qui doit souscrire à deux polices aux conditions différentes pour tenter de garantir l'uniformité de sa couverture, avec un succès parfois mitigé. Pour l'entreprise elles apportent un sentiment de sécurité trompeur car elles n'offrent souvent qu'une protection lacunaire contre les sinistres cyber qui se retrouvent exclus des polices standards. De plus elles n'indemnisent qu'à un niveau bien inférieur au besoin potentiel de l'entreprise, comme si l'impact des sinistres cyber devait par nature être inférieur à ceux des sinistres classiques.

Le besoin de l'entreprise tel que nous l'avons identifié est de disposer d'une couverture recouvrant uniformément l'ensemble de la menace qui pèse sur elle et garantissant une indemnisation à la hauteur du préjudice potentiel associé. Elle devra être construite à partir de briques adaptées à la morphologie spécifique de son profil de risque. S'il est vrai que certains risques et types de sinistres sont apparus du fait de la numérisation et justifient donc la mise en place de nouvelles polices cyber spécifiques, l'impact du cyber sur les risques existant préalablement ne doit pas être traité par une exclusion de ceux-ci des polices traditionnelles même quand ils sont intensifs en capitaux. L'assureur peut s'inquiéter à juste titre d'un défaut d'investissement en cyber sécurité mais plutôt que de s'en désolidariser, il lui faut inciter et accompagner le développement de cet investissement.

VI. Les défis posés aux assureurs

Le rôle que doit tenir l'assureur pour accompagner la transformation numérique des entreprises requiert une expertise qui lui fait encore défaut dans le cas du cyber. Il lui faudra donc surpasser les difficultés liées aux problématiques de ressources humaines afin de monter en compétence et être en mesure de dialoguer avec ses clients et de les conseiller, non seulement dans le choix de la solution assurantielle la mieux adaptée, mais aussi dans leur gestion du risque.

Il lui faudra réviser ses méthodes de travail face à un risque récent et évolutif pour lequel les données actuarielles sont rares et trouver une parade au risque de cumul qu'il engendre.

Enfin dans un monde en mutation permanente, il ne devra pas négliger sa propre transformation numérique et même aller jusqu'à anticiper les évolutions potentielles de son marché en particulier dans le domaine du droit de la responsabilité.

La menace du manque de compétence et de données

Afin de jouer efficacement le rôle que nous avons précédemment identifié comme souhaitable, l'assureur doit impérativement être capable d'engager un dialogue constructif avec son client. En particulier il doit donc être en mesure de comprendre les problématiques de sécurité numérique associées à son risque et être à même d'exploiter ses propres atouts pour y apporter des propositions de solutions. Or chez la plupart des assureurs et réassureurs que nous avons eu l'occasion de rencontrer, les compétences cyber sont identifiées comme faisant défaut : c'est le premier obstacle au développement d'une bonne compréhension du risque. Il est en effet crucial que les acteurs de l'assurance parviennent à construire l'expertise technique sous peine de se retrouver incapables de communiquer avec les entreprises et donc a fortiori de se développer sur un marché duquel ils pourraient finir par être exclus, remplacés par d'autres acteurs nés de la numérisation et mieux équipés pour traiter ces sujets.

Cependant de nombreux assureurs admettent une certaine impuissance face à la problématique de ressources humaines que cette montée en compétence implique nécessairement. La pénurie d'experts du numérique engendre une difficulté à recruter du personnel qualifié dans ce domaine à laquelle s'ajoute celle de les faire travailler efficacement en collaboration avec les métiers traditionnels de l'assurance. En effet, ceux-ci sont habitués, de par la culture liée à leur activité, à une certaine dynamique souvent en contradiction avec celle qui s'est développée chez l'assureur.

Souvent très mobiles, ils sont attachés à l'innovation, l'optimisation des procédés, s'attendent à un épanouissement permanent et recherchent des évolutions de carrière rapide. Ils ne sont donc pas toujours compatibles avec le rythme plus mesuré, méthodique et précautionneux du domaine l'assurance. Cet écart de personnalité est une réelle problématique pour les départements « cyber » qui cherchent à construire une expertise interne en la matière mais peinent à constituer une équipe cohérente ou à la maintenir en place plus longtemps que quelques années. Ils ont ainsi du mal à construire ou adapter leurs modèles internes ainsi qu'à auditer leurs clients et doivent donc souvent se résoudre à recourir à des prestataires extérieurs ou à acquérir des sociétés spécialisées sur le sujet et à qui ils confient cette expertise.

Un défi pour les méthodes actuarielles

Afin d'être pertinent dans son rôle de conseil et d'apporter une réelle plus-value à son client, l'assureur doit également être en mesure d'appréhender correctement le risque. La méthode traditionnelle consiste à s'appuyer sur un historique actuariel, une base de données décrivant les occurrences des sinistres passés et permettant de construire des modèles statistiques prédictifs garantissant la rentabilité de l'activité d'assurance sur le long terme. Or dans le cas du risque cyber, un tel historique n'existe pas et pourrait ne pas exister avant longtemps pour un certain nombre de raisons :

- Tout d'abord il s'agit d'un risque qui ne s'est développé que très récemment, les premiers virus datant des années 90 et les premières attaques cyber n'ayant fait leur apparition qu'il y a une douzaine d'années. Cette échelle de temps peut sembler significative mais elle est extrêmement courte en comparaison de l'historique développé sur les autres risques que couvre l'assurance. De plus la démarche de collecte de données de sinistralité n'a en fait été entamée par l'assureur qu'il y a quelques années, longtemps après l'apparition des premiers risques.
- Ensuite le risque est pour l'instant extrêmement évolutif. La guerre des virus contre antivirus a incité les deux camps à continuellement innover afin de trouver de nouvelles méthodes, pour l'un d'intrusion et de nuisance, pour l'autre de détection et de protection. Les produits informatiques et les standards de communication par internet sont par ailleurs en constante évolution pour s'adapter aux évolutions des usages et du marché mais cela génère au passage un constant renouvellement de failles qui offrent aux attaquants autant d'opportunités d'exploiter la confiance que l'utilisateur

place en ces produits. Il n'est cependant pas exclu que les techniques finissent par se stabiliser. On voit en effet déjà émerger certaines grandes tendances, le « cheval de Troie » et le « phishing » restant toujours après de nombreuses années parmi les procédés les plus largement répandus.

- Probablement du fait des deux raisons précédentes, aucun langage commun n'a pu se développer pour l'instant entre les différents acteurs, qui sont donc incapables de parler du cyber à partir des mêmes bases. Ceux-ci ne s'entendent pas sur les définitions et la classification des différents vecteurs de risques ni au sujet de leurs conséquences et des caractéristiques techniques importantes à leur étude. Sans l'établissement d'un vocabulaire commun, aucun partage d'information et d'historique entre assureurs ne sera possible car chacun a développé des conceptions propres du risque incompatibles entre elles.
- Enfin on constate globalement un taux de déclaration de sinistres cyber par les entreprises assez faible. Que cela soit par souci de confidentialité, désintérêt, ou simplement méconnaissance du caractère cyber du sinistre, cette rareté de la remontée d'information ralentit la constitution d'une compréhension du sujet mais compromet également l'éventuelle mise en place d'une plateforme publique de collecte de donnée pour des raisons de confidentialité. En effet, une base de données, même statistique, ne peut pas garantir l'anonymat de ceux qui y participent si ceux-ci sont trop peu nombreux.

Un marché qui réveille les appétits

Outre les assureurs, le marché de la prévention et de la gestion du risque cyber pourrait être convoité par plusieurs acteurs qui ont aussi de leur côté bien identifié l'opportunité de croissance à se placer sur une chaîne de valeur nouvelle et en plein développement.

- Les courtiers, grâce à leur relation directe et privilégiée avec les clients commencent déjà, pour certains, à imposer des « intercalaires », contrats standards, aux assureurs et tentent donc de décider de la forme que prendra la couverture assurantielle de demain. Le rôle d'intermédiaire qu'ils jouent déjà et le rapport de force avantageux qu'ils entretiennent avec les assureurs pourraient leur permettre de se placer également sur le segment de la prescription de solutions de cyber sécurité.
- Les prestataires de sécurité, de leur côté, cherchent naturellement à étendre leur activité afin de couvrir non seulement la protection contre le risque cyber

mais également sa détection, sa prévention et sa remédiation. En utilisant leur connaissance de la menace, ils peuvent également construire des modèles d'estimation du niveau de risque des assurés ou de gestion des cumuls et ainsi préempter un segment habituellement réservé à l'assurance.

- Bien que cela ne soit pas leur cœur de métier, les GAFAM (ces grands groupes américains, *Google*, *Amazon*, *Facebook*, *Apple* et *Microsoft*) disposent des compétences techniques pour s'imposer sur les marchés de la prévention et des capitaux suffisants pour être en mesure de se placer également sur le secteur de l'assurance s'ils estiment que leur avantage compétitif leur permettrait d'y être rentable sans trop s'exposer. De plus l'importante base d'utilisateurs de leurs produits existants leur permettrait de pénétrer ce marché très rapidement.

Des atouts solides pour rattraper le retard

L'assurance est en retard par rapport à ces acteurs sur le plan technique mais dispose toutefois de certains atouts. Elle effectue tout d'abord un suivi personnalisé des besoins de ses clients, en particulier des PME, et dispose donc d'une bonne connaissance de leur profil de risque au-delà du simple aspect cyber. Or nous avons montré qu'il était important, pour correctement appréhender l'impact du cyber, de prendre en compte l'ensemble du profil de risque des entreprises. De plus elle est très solvable et n'est pas contrainte par la nécessité de rendements rapides ou importants, l'activité d'assurance étant par nature très intensive en capitaux, et peut donc s'imposer. Plusieurs stratégies s'offrent donc à elle :

- S'appuyer sur des partenariats, plutôt nombreux et diversifiés que stables, afin d'exploiter certaines synergies, récupérer les données de sinistralité qui lui manquent et exploiter des compétences dont se doter requerrait un temps important.
- S'imposer comme prescripteur d'offres de solutions de gestion de crise et de remédiation chez les clients existants et garantir ainsi leur réaction efficace à un sinistre cyber. En jouant le rôle d'intermédiaire entre son client et les divers prestataires de sécurité, l'assureur garantit l'efficacité de ces derniers en animant une saine concurrence. En revanche si l'entreprise est en mesure de choisir un prestataire, l'assureur devra respecter ce choix et rester en mesure de compléter la protection souscrite par une couverture assurantielle.
- Se substituer au *risk management* dans les petites entreprises. Chez celles-ci les profils de risques critiques restent assez standards au sein d'un même secteur d'activité et l'assureur pourrait donc proposer des scénarios

dimensionnants construits sur la base des problématiques identifiées sur la masse de sa clientèle. Il serait alors en mesure d'offrir des briques assurantielles sur mesure permettant au client de construire la couverture qu'il estime adaptée à son besoin en fonction de son budget et de son aversion au risque. Cette démarche permettrait également de mettre en évidence la nécessité d'une gestion du risque et constituer une incitation à la gouvernance en interne.

- Développer l'offre de prévention pour répondre à la menace des GAFAM et capter une partie de la valeur associée tout en gardant les activités de gestion et le risque capitalistique. Accompagner le client vers une prévention efficace du risque cyber est un enjeu important de l'assureur et un rôle qu'il remplit déjà dans le cadre des autres risques via le cercle vertueux théorique de l'assurance. Toutefois il s'agira de rester réaliste quant à la capacité actuelle à systématiser la prévention. Aujourd'hui une partie non-négligeable des sinistres provient d'erreurs humaines de sorte que les premiers visés devraient être les processus humains.

Réinventer ses méthodes de travail face à un risque nouveau

Les méthodes actuarielles traditionnelles sont inadaptées pour traiter le risque cyber faute d'historique suffisant. Ce problème est à l'origine de la mauvaise compréhension du risque cyber par l'assureur et la grande incertitude qu'elle engendre constitue un des freins majeurs au développement de ce marché. Un sujet clé pour l'assureur consiste donc à adapter ses méthodologies d'estimation du risque pour prendre en compte les caractéristiques propres à ce nouveau risque. Une première solution pourrait consister à partir des modèles existant pour les autres risques, puisque l'on a démontré que le cyber était avant tout une modification des profils de risques déjà couverts.

Il pourrait alors simplement s'agir dans un premier temps d'isoler les paramètres susceptibles d'être impactés par le cyber et faire ainsi coller au mieux ces modèles à la sinistralité observée ou anticipée en gardant à l'esprit que l'impact du cyber reste encore peu visible et que la numérisation a même tendance à tirer cette sinistralité à la baisse. Plutôt que les données, utiliser l'expertise permettrait de prendre en compte les spécificités de ce risque et de les intégrer aux modèles connus en gardant toutefois en tête que la menace est évolutive et susceptible de changer radicalement à chaque innovation technologique.

Le risque cyber, du fait de la standardisation des outils et de l'interconnexion des acteurs économiques, particuliers et institutionnels peut revêtir une composante systémique. Une même faille ou une même attaque pourraient conduire à des conséquences étendues et d'ordre catastrophique. Un enjeu de l'assureur est donc de mesurer précisément son exposition, en particulier du fait des *silent covers*, afin de garantir sa solvabilité. Pour lutter contre cet aspect, il lui faudra gérer la diversification de son portefeuille en conséquence en y intégrant suffisamment de clients peu exposés du fait de leur cœur de métier, de leur faible connectivité ou encore de la rusticité de leurs procédés. Il faudra notamment tirer parti des différences sectorielles et ne pas complètement ignorer les effets géographiques qui existent aussi dans le cas du cyber non pas du fait de la diversité de la menace mais du fait de la diversité des standards de logiciel et de communication, des niveaux de protection, etc.

Le réassureur moteur de la bonne santé du marché

Le réassureur a un rôle important à jouer dans la maîtrise de cet aspect systémique. Pour garantir sa solvabilité il lui faudra engager ses clients assureurs à maîtriser leurs cumuls internes et vérifier que la diversité et la décorrélation de leurs portefeuilles respectifs permet bien une mutualisation efficace. En particulier il lui faudra prendre en compte la structuration du marché des grands risques en « tours d'assurance ». Les assureurs inquiets de leur exposition à un risque qu'ils ne comprennent pas préfèrent souscrire une multitude de petits contrats plutôt que de s'engager sur de gros montants auprès d'un unique client.

Ainsi les entreprises qui cherchent à se couvrir pour des montants importants ont besoin de faire appel à plusieurs assureurs, le premier indemnisant les frais excédant directement le montant de la franchise jusqu'à une certaine limite, le second indemnisant les frais excédant cette limite jusqu'à un second plafond et ainsi de suite. La frilosité des assureurs est cependant telle que l'entreprise doit parfois aller jusqu'à requérir la participation de presque tous les assureurs principaux du marché entraînant ainsi une forte corrélation entre ces acteurs. Si un sinistre venait à impacter un grand nombre d'entreprises assurées de cette façon, tous les assureurs seraient mis en défaut de paiement en même temps et feraient simultanément appel à leur réassureur qui ne serait pas en mesure de faire face.

On peut cependant trouver des raisons de chercher à modérer cette vision catastrophique du risque systémique. Déclencher une attaque touchant des acteurs partout dans le monde et engendrant de grandes pertes assurables reste aujourd'hui du domaine de l'incertain, relevant d'attaquants d'une motivation très importante et

dont l'objectif reste à trouver. Les scénarios de déstabilisation de l'ordre mondial relèvent d'une autre catégorie de risques que les sinistres plus circonscrits pour lesquels l'assurance à toute sa place.

Anticiper les évolutions du droit de la responsabilité

L'apparition de nouvelles technologies et usages numériques comme le développement récent de l'« Internet des Objets » (ou IoT pour *Internet of Things*) remet en cause la chaîne de responsabilité relative à la propriété des choses. Des objets du quotidien deviennent automatisés, connectés voire « intelligents ». On constate ainsi le déploiement de produits possédés par des utilisateurs qui ne sont pas en mesure d'en exercer un contrôle direct. Ce contrôle peut maintenant être effectué par un opérateur distant ou délégué automatiquement à un programme informatique intégré.

Ces nouveaux objets ont le potentiel de révolutionner et de modifier en profondeur les niveaux de risque portés par les différents maillons de la chaîne de valeur associée. Un dégât pouvait jusqu'alors survenir du fait d'une mauvaise utilisation de l'objet ou d'un défaut de fabrication. A présent il faudra s'attendre à des dysfonctionnements pouvant provenir de la conception ou de la fabrication des composants, des logiciels pilotes ou de sécurité, de l'intégration de l'objet à son environnement, de l'opérateur en charge de la gestion de l'objet et toujours, mais plus rarement, de l'utilisateur lui-même qui se retrouve déresponsabilisé. Ce nouveau modèle aura nécessairement un impact sur la rentabilité de l'assurance dans la mesure où il tend à être paradoxalement plus sûr, chaque acteur étant responsable d'un segment plus court, et donc à diminuer la sinistralité.

Selon les modèles d'affaires qui se mettent en place, le marché des assureurs pourrait alors être réduit mécaniquement par ces innovations. Prenons l'exemple de la voiture autonome, dont l'assurance constitue le premier marché assurantiel hors assurance vie : aujourd'hui les utilisateurs possèdent leur voiture, l'utilisent 2 à 3% du temps seulement et sont responsables de leurs accidents (s'ils en sont à l'origine) ; ces trois assertions pourraient être remises en cause par l'introduction de la voiture autonome avec des impacts potentiels évidemment très forts (diminution de la taille du parc de véhicules, baisse de la sinistralité).

Une possible mutation de la responsabilité générale

Ce modèle modifie également la chaîne de responsabilité associée aux différents maillons et devrait donc à terme impacter le segment « responsabilité civile » de

l'assurance. En effet, selon les évolutions à venir du droit de la responsabilité, il se pourrait que l'assureur n'ait plus besoin de couvrir l'utilisateur mais un ou plusieurs autres acteurs de la chaîne de valeur. Pour l'instant il existe très peu de jurisprudence sur le sujet, la loi laissant encore à l'utilisateur final la responsabilité des objets qu'il « contrôle » au sens juridique du terme. Si l'on reprend l'exemple de la voiture autonome, il y a fort à parier que l'assureur ne pourra plus se contenter d'assurer les conducteurs. On pourrait imaginer qu'il couvre à la place un éventuel opérateur chargé de l'entretien, la gestion et la surveillance d'une flotte de véhicules. Il pourrait aussi assurer l'intégralité de la chaîne de fabrication ou encore les véhicules eux-mêmes mais pourra-t-on alors encore parler de responsabilité civile dans la mesure ou un objet ne saurait être tenu responsable ?

De nos discussions avec des avocats portant sur les questions relatives aux nouvelles technologies numériques, il ressort que les régimes de responsabilité en place sont robustes et que le droit positif n'a pas de raison d'évoluer. Les modèles d'affaires qui émergeront et la jurisprudence participeront à définir si un objet intelligent, un robot, une voiture autonome relèvent davantage du régime de responsabilité de la possession des animaux que de celle des choses. Plus particulièrement en ce qui concerne la voiture, il nous paraît nécessaire pour l'assureur d'être actif dans les discussions et d'anticiper l'évolution d'un de ses plus gros marchés.

Réussir sa transformation numérique interne

L'assureur doit également mener de front sa propre transformation numérique. Dans la démarche d'estimation du risque, notamment cyber, de ses clients il peut être amené à disposer d'informations confidentielles qui pourraient faire de lui une cible privilégiée et doit en conséquence s'équiper d'un système d'information au moins aussi sécurisé que celui des entreprises qu'il assure.

Le cœur de métier traditionnel de l'assurance reste très intensif en ressources humaines et offre de multiples opportunités de tirer parti de la numérisation pour améliorer sa productivité. La transparence et la réactivité que peuvent apporter à moindre coût les outils numériques seront cruciales pour améliorer les services de conseil, de suivi, de relation client fournis qui accompagnent la couverture elle-même.

L'assureur ne peut plus se permettre de se reposer exclusivement sur les connaissances qu'il est capable de constituer en interne de par les données de sa clientèle et son expertise propre. Il doit développer une capacité à créer des partenariats et à exploiter des nouvelles sources de données et de connaissances sous

peine de voir une partie de sa valeur ajoutée captée par des acteurs plus agiles tels que les GAFAM.

Enfin d'autres acteurs clés de la chaîne de valeur de l'assurance doivent également se restructurer. Les entreprises de certification par exemple prennent des engagements sur l'avenir et la résilience future de certains produits, procédés ou sites industriels. Dans le cadre de produits logiciels ou informatisés, il est aujourd'hui difficile d'aller au-delà de la certification de processus de management. Alors que l'obtention d'un certificat technique suffisait à rassurer l'assureur quant à la fiabilité d'un produit pour qu'il s'engage à le couvrir, pour des produits numériques, le certificateur ne peut désormais garantir que le bon passage de certains tests correspondant aux risques connus à un instant donné. Il ne sera plus en mesure de promettre une robustesse à long terme d'un produit face à des menaces en constant renouvellement.

VII. Le rôle de la puissance publique

Le marché de l'assurance n'a pas besoin de contraintes réglementaires supplémentaires pour prendre le virage de la transformation numérique. Certains points de droit gagneraient à être réaffirmés pour éviter les distorsions de concurrence, comme l'inassurabilité des rançons et des amendes. Une réflexion de niveau européen sur la déresponsabilisation des prestataires de services de cloud est à mener vu le risque systémique qu'ils font porter à notre économie.

A l'image du Royaume-Uni, le régulateur peut jouer un rôle central dans la structuration du marché, en levant l'incertitude sur l'exposition prise par les assureurs dans leurs polices n'excluant pas les faits générateurs cyber (*silent covers*) et en animant les débats aux côtés des fédérations d'assureurs et de réassureurs et de l'ANSSI sur la standardisation des exclusions et l'établissement de normes de niveau de sécurité.

La création d'une assurance obligatoire ou d'une garantie de dernier ressort de l'État n'est pas pertinente pour la couverture de scénarios qui relèvent du risque d'entreprise et du risque juridique davantage que de la protection des individus et de leur propriété. La montée en compétence des assureurs sur les risques cyber et leur cumul palliera leur manque d'appétit.

En tiers de confiance indépendant et à travers le groupement d'intérêt public ACYMA nouvellement créé, l'État est positionné pour jouer un rôle de plateforme, à des fins d'observatoire du risque en mutualisant les données de sinistre et d'assistance aux sinistrés en les mettant en relation avec les prestataires de gestion de crise et de remédiation adéquats.

En tant que jeunes fonctionnaires, nous nous devons d'adresser nos recommandations aux pouvoirs publics au sens large. Leur absence de notre discours jusqu'à présent se justifie par la volonté de ne pas imposer de contraintes réglementaires supplémentaires sur un marché encore en devenir. Nous nous sommes efforcés de proposer des leviers d'action plus souples visant à sensibiliser les acteurs, entreprises et assureurs principalement, aux défauts d'optimalité que nous observons avec un regard externe et dénué d'intérêts commerciaux. Au-delà de cette *soft-regulation*, nous identifions des points particuliers où l'État a un rôle à jouer.

Réaffirmons le droit

Sans besoin de législation nouvelle, des points de droit soumis à interprétation méritent d'être réaffirmés.

Rançons et amendes

Concernant les rançons, leur paiement peut participer du financement du terrorisme et est donc illicite en France. Elles ne peuvent dès lors pas faire partie de garanties couvertes par un contrat d'assurance. Par ailleurs, s'il peut paraître économiquement intéressant de payer lorsque l'on est confronté à une extorsion sur des données vitales à l'entreprise, on ne dispose d'aucune garantie quant à la récupération de ces données après paiement, ni quant à la non-réplicabilité du sinistre dans les jours qui suivront. Le bon équilibre économique réside en réalité dans la prévention, grâce à l'établissement de processus de sauvegarde régulière sur des supports déconnectés du réseau, de reprise d'activité pour remplacer rapidement les données manquantes après un sinistre et de tests réguliers (intégrité des sauvegardes et efficacité du plan de reprise).

Il en va de même pour les amendes, qu'elles soient pénales ou administratives. Relevant d'une faute vis-à-vis de la réglementation, elles constituent un risque illicite, et parfois jugé volontaire, donc ne pouvant relever de l'assurance. Ces amendes représentent un levier de dissuasion contre une action non-conforme à la législation et leur prise en charge par un autre acteur que le fautif les viderait de leur substance punitive.

L'affirmation des règles de droit sur ces points précis permettrait de limiter la distorsion de concurrence engendrée par certains assureurs proposant ces garanties comme produit d'appel dans des contrats de portée mondiale tout en restreignant, plus discrètement, leur action aux territoires où elles sont légales.

Clauses contractuelles abusives

Sur un sujet connexe à l'assurance des risques cyber qui émerge dès que l'on s'intéresse à la gestion des cumuls, une réflexion gagnerait à être menée au regard de clauses contractuelles abusives faisant planer un risque systémique sur notre société. L'externalisation des services informatiques des entreprises vers des prestataires de type *cloud* est une tendance profonde de la dernière décennie. Ils permettent une réduction des coûts d'infogérance ainsi qu'un gain en sécurité : les prestataires mutualisent les risques de gestion informatique d'un grand nombre d'entreprises et investissent efficacement pour s'en prémunir à travers la redondance, le maintien à

jour logiciel et matériel et des systèmes de surveillance et de défense à un niveau qu'une entreprise seule ne pourrait assumer. Cette concentration des risques fait en revanche peser un risque systémique : une indisponibilité des services des grands prestataires de cloud engendrerait un arrêt d'exploitation de la plupart de leurs clients qui sont devenus dépendants de ces services. Ces grands prestataires utilisent par ailleurs leur position dominante pour imposer des clauses contractuelles, sans négociation possible de la part des entreprises clientes qui « acceptent » des conditions générales d'utilisation des services en cochant la case adéquate en bas de la page, visant à se déresponsabiliser de toute indisponibilité, destruction ou perte de confidentialité des données des clients[12]. Alors même que la profession d'assureur est fortement réglementée pour encadrer le risque systémique qu'il ferait porter à la société en cas d'insolvabilité, on peut légitimement s'interroger sur l'absence de réglementation de ces acteurs au titre du risque systémique qu'ils engendrent. Les prestataires dominants étant de manière générale des sociétés américaines, le bon échelon de réflexion pour aborder ce problème nous semble être le niveau européen.

Un rôle moteur pour le régulateur dans l'assainissement du marché

Exposition silencieuse : les silent covers

De nos discussions avec l'ACPR (Autorité de Contrôle Prudentiel et de Résolution), nous retenons que les problématiques de solvabilité des assureurs liées aux risques cyber ne sont pas jugées de taille suffisamment importante pour être abordées par le régulateur français aujourd'hui. La taille du marché représenté par les offres cyber spécifiques est en effet négligeable devant celle des autres lignes d'assurance. Or nous avons observé que l'ensemble des couvertures assurantielles d'une entreprise peut être déclenché par un sinistre de cause cyber. Dans tous les contrats de type « tous risques » où ces faits générateurs cyber ne sont pas spécifiquement exclus, les assureurs portent donc une exposition au risque cyber.

Cette exposition, dénommée *silent coverage* en anglais en opposition à une souscription cyber dédiée nommée *affirmative coverage*, a été identifiée comme problématique par le régulateur britannique, le PRA (*Prudential Regulation Authority*) [10] [11]. En conclusion des travaux d'analyse menés entre octobre 2015 et juin 2016, le PRA a alerté les assureurs et réassureurs quant au manque de garanties qu'ils fournissent sur leur bonne prise en compte de cette exposition

[12] Voir à titre d'exemple les chapitres 10. Exonérations de responsabilité et 11. Limitations de responsabilité du Contrat client AWS - https://aws.amazon.com/fr/agreement/

croissante dans le temps dans leurs modèles actuariels. L'investissement en compétences et en stratégie sur le sujet sont jugés comme insuffisants en comparaison des enjeux, même chez les assureurs souscrivant des contrats dédiés aux risques cyber.

Pour lever l'incertitude régnant sur cette problématique de *silent coverage*, les avis des différents acteurs mentionnant tour à tour un non-sujet et une catastrophe dormante, nous recommandons au régulateur d'agir en imposant aux assureurs et réassureurs une démonstration de leur exposition aux risques cyber dans leurs polices déjà souscrites, qu'elles soient orientées cyber ou non.

Nous pensons que cette action participera à l'assainissement en profondeur du marché. En effet, le meilleur moyen pour l'assureur d'estimer son exposition est d'instaurer un dialogue avec son client autour des scénarios cyber critiques pour l'entreprise qui peuvent déclencher les polices d'assurance souscrites. Les entreprises les plus matures engageront alors une révision de leurs polices pour couvrir au mieux ces scénarios, les entreprises les moins matures seront sensibilisées à la nécessité de la construction de ces scénarios.

Exclusions et Standards de sécurité

Au-delà des considérations purement réglementaires, le régulateur peut être moteur sur les réflexions concernant la standardisation des exclusions et des normes, aux côtés des fédérations d'assureurs et de réassureurs comme la FFA (Fédération Française de l'Assurance) et l'APREF (Association des Professionnels de la Réassurance en France) - principaux organes de concertation du marché - et l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), garant étatique de la compétence en cyber sécurité.

Nous avons précédemment décrit la mutualisation du risque portée par les prestataires de *cloud*. De manière plus générale, les services de réseau comme l'électricité et les télécommunications, utilisés par un grand nombre d'acteurs économiques, font porter un risque systémique difficilement endossable par les assureurs. Ce risque freine l'appétit de ces derniers et gagnerait à être exclu des couvertures assurantielles au profit de clauses contractuelles plus favorables aux clients de ces prestataires de services. D'autres types d'exclusions pourraient faire partie d'un processus de standardisation, comme celles limitant les garanties cyber actuellement silencieuses des contrats non-cyber. L'objectif d'un tel processus de standardisation est de rendre les contrats plus lisibles, comparables, juridiquement plus forts et opposables aux négociations farouches des courtiers. Un tel processus a

été observé sur les places de marché anglo-saxonnes[13], mis en œuvre principalement par la *Lloyd's Market Association* (UK) et l'*Insurance Services Office* (US).

Un autre point où une réflexion de place de marché trouverait son intérêt est dans l'émergence de standards de niveaux de sécurité permettant de discriminer les entreprises selon leur maturité en prévention et en réaction aux risques cyber. Cette discrimination est ce qui permet aux assureurs d'ajuster les primes des polices d'assurance en fonction du niveau de risque représenté par l'entreprise, donc de les inciter à investir en sécurité préalablement à la souscription d'une assurance. Là où la France se contente de sensibilisation et de recommandations à travers les bonnes pratiques supportées par l'ANSSI [12], le Royaume-Uni a poussé la démarche plus avant en développant un standard de sécurité certifiant nommé *Cyber Essentials* [13]. Sans préjuger de la qualité de ce standard qui continue d'évoluer et de se complexifier, il est aujourd'hui utilisé en prérequis à la souscription de la plupart des offres d'assurance britanniques ayant une dimension cyber. L'établissement de telles normes est un véritable défi quant à leur contenu afin d'inclure des considérations techniques, de politique de sécurité, de processus de gestion des risques, des évolutions et des différentes échelles d'applicabilité. Cela nous paraît cependant être un effort bénéfique à la sensibilisation des entreprises au chemin qu'elles doivent suivre pour gérer efficacement leurs risques.

L'État doit-il se porter garant ?

Le sujet de l'État garant intervient dans deux situations :

- Lorsque l'on juge que l'indemnisation d'un sinistre doit intervenir rapidement et de manière certaine afin de protéger les victimes de dommages corporels, parfois matériels, indépendamment de la recherche et de la poursuite d'un éventuel responsable aux conditions de solvabilités douteuses. Ce cas est intimement lié au concept d'assurance obligatoire. Illustrons ceci par l'exemple de l'assurance en responsabilité des conducteurs de véhicules terrestres motorisés. Les victimes d'un accident de la route sont indemnisées pour leurs dommages corporels, soit par l'action de l'assurance

[13] Voir les principales exclusions britanniques de la Lloyd's Market Association (NMA2912, NMA2914, NMA2915, LMA3030), la très large "CL380 - Institute cyber attack exclusion clause" ou encore "Exclusion - Access Or Disclosure Of Confidential Or Personal Information And Data-Related Liability - Limited Bodily Injury Exception Not Included" de l'Insurance Services Office (ISO) pour le marché US.

obligatoirement contractée par le conducteur responsable identifié, soit par l'action du fond de garantie des assurances obligatoires de dommages (FGAOD) si le conducteur responsable n'est pas identifié ou si son assurance n'est pas valide. Ce fond de garantie est financé par les assurés et les assureurs via des contributions obligatoires et, s'il venait à être non solvable, par l'État. Sans assurance obligatoire cette fois-ci mais via une contribution prélevée sur tous les contrats d'assurance des biens, les victimes d'actes de terrorisme font l'objet d'une indemnisation pour les dommages corporels via le fond de garantie des victimes des actes de terrorisme et d'autres infractions (FGTI).

- Lorsque l'on juge nécessaire pour la protection de la propriété des individus qu'ils soient indemnisés lors de sinistres, qui de par leur ampleur et leur fréquence imprévisibles ne pourraient être couverts de manière économiquement viable par le marché d'assurance. C'est le cas des catastrophes naturelles et des actes terroristes, pour lesquels l'État apporte des capacités de réassurance illimitées de dernier ressort via la Caisse Centrale de Réassurance (CCR). Dans le cas du terrorisme, les assureurs mutualisent la gestion de leur réassurance pour les contrats dommage aux biens en adhérant au GAREAT (Gestion de l'Assurance et de la Réassurance des risques Attentats et actes de Terrorisme) : si les capacités de réassurance de ce pool de marché s'épuisent, c'est-à-dire si le seuil d'intervention de l'État est atteint, le traité de réassurance illimité avec la CCR entre en action.

Dans aucun de ces contextes nous ne parvenons à définir un cadre où la garantie de l'État serait pertinente vis-à-vis des risques cyber. D'une part, si des actes de terrorisme utilisant des méthodes numériques venaient à engendrer des dommages corporels et matériels, les mécanismes en place interviendraient nominalement. D'autre part, bien que l'appétit des assureurs pour les risques cyber soit aujourd'hui freiné par la peur d'un risque systémique, il ne nous paraît pas concevable que l'État intervienne en garantie d'un risque d'entreprise ou pire, d'un risque juridique : pertes d'exploitation suite à l'indisponibilité des systèmes informatiques, défaut de protection du capital informationnel de l'entreprise, obligation de notification des utilisateurs suite à une fuite de données personnelles… L'équilibre économique doit être trouvé par une gestion intelligente des cumuls bien davantage que par l'intervention de l'État qui introduirait par ailleurs des biais négatifs sur l'appétit au risque : certains territoires à risque seraient par exemple nettement moins bâtis si l'État ne garantissait pas l'indemnisation en cas de catastrophe naturelle.

Un rôle de tiers indépendant : l'État plateforme

En écho au mémoire de nos camarades Laura Létourneau et Clément Bertholet titré *Ubérisons l'État ! Avant que d'autres ne s'en chargent* [14], nous identifions des objectifs pour lesquels un tiers de confiance indépendant serait bénéfique à l'intérêt général : nous proposons ici que ce rôle soit rempli par l'État.

Le premier objectif réside dans une mutualisation des données de sinistres. Les entreprises connaissent les attaques qui les touchent spécifiquement, les prestataires de sécurité connaissent les types de menaces et leur fréquence, les assureurs connaissent les quelques sinistres payés dans les premières années de balbutiement du marché, la justice connaît les plaintes déposées. Aucun acteur n'est en mesure de cerner en globalité l'état de la menace et de ses conséquences avérées dans les entreprises. D'une part, ce manque de visibilité donne un avantage considérable aux attaquants qui profitent du temps de réaction nécessaire au partage des recommandations de sécurité entre toutes les entreprises. D'autre part, il empêche le marché d'assurance de se structurer sur des bases actuarielles crédibles. Le Royaume-Uni remplit cet objectif grâce à un observatoire du risque cyber, créé en 2013, nommé CiSP (*Cyber Security Information Sharing Partnership*) [14], qui centralise les données de sinistre déclarées par les entreprises et les relaye aux industries qui en ont besoin.

Le second objectif est d'aider l'ensemble des entreprises à faire face aux crises générées par des sinistres cyber. Nous avons identifié que la gestion de la crise est critique sur l'ampleur du sinistre et qu'en particulier pour les plus petites entreprises, certains sinistres mal gérés peuvent mener jusqu'au dépôt de bilan. Beaucoup d'entreprises sinistrées sont complètement démunies sur les démarches à accomplir jusqu'à leur reprise d'activité, qu'elles soient techniques (remise en état du système informatique) ou administratives (dépôt de plainte, déclenchement d'assurance). Une plateforme à destination des entreprises qui n'ont pas la taille critique pour gérer leur crise de manière autonome permettrait de les guider dans ces démarches et en particulier de les mettre en relation avec des prestataires de gestion de crise et de remédiation. Des avis laissés par les autres entreprises sinistrées par le passé permettront de discriminer les prestataires selon leur spécialité et leur compétence, donnant ainsi accès au service le plus pertinent pour l'entreprise en crise.

[14] Voir https://www.ncsc.gov.uk/cisp pour plus d'informations sur cette instance

Ces deux objectifs sont portés par un groupement d'intérêt public récemment créé et incubé au sein de l'ANSSI. Il se nomme GIP ACYMA (Actions contre la CYberMAlveillance)[15] et teste depuis juin 2016 une plateforme numérique dans la région Hauts-de-France pour recueillir les données de sinistre et diriger les entreprises sinistrées vers les prestataires adéquats.

[15] Voir la Convention constitutive du groupement d'intérêt public pour le dispositif national d'assistance aux victimes d'actes de cybermalveillance - https://www.ssi.gouv.fr/uploads/2017/01/gip-acyma.pdf

Conclusion

Par nature difficile à appréhender, le risque cyber ne laisse pas indifférent et souvent, il divise. Anecdotique pour certains, évidemment à l'origine de la prochaine catastrophe de grande ampleur pour les autres, il a souvent été endossé de manière partiellement consciente par des acteurs économiques qui cherchent désormais à le transférer en partie à l'assurance.

Si le terme d'« assurance des risques cyber » laisse à penser que la solution miracle existe sous la forme d'un seul produit, la réalité nous semble davantage relever d'une adaptation de toutes les branches de l'assurance à la révolution numérique. Au prix d'un effort de segmentation par taille d'entreprise et secteur d'activité, on comprend que ce qui est critique pour l'un est bénin pour l'autre. Toutefois, du dommage corporel au conseil juridique, aucun type de prestation n'est épargné par le risque cyber : l'assurance à un rôle clé à jouer dans l'accompagnement des entreprises dans leur transformation numérique.

Pour faire progresser le niveau de sécurité et renforcer la résilience du tissu économique, dans les entreprises mais également chez les assureurs, l'heure est grandement venue du diagnostic afin que « cyber » ne soit plus synonyme de « zone d'ombre ». Dans les entreprises, l'enjeu est dans la mise en place d'une gouvernance permettant de s'approprier les scénarios critiques de risque, pour les comprendre, les prévenir et éventuellement transférer le risque résiduel. Chez les assureurs, l'explicitation des garanties est la clé pour la mesure de leur niveau d'exposition et une diversification habile. La gestion des compétences et l'anticipation de l'évolution des usages sont des défis majeurs pour être en mesure d'assumer leur rôle sur le long terme.

La puissance publique ne nous semble pas devoir intervenir aujourd'hui sur ce marché en pleine construction pour légiférer ou se porter garante. Son rôle est davantage bénéfique en tant que tiers de confiance, à travers des plateformes de partage, ainsi qu'en tant qu'animateur des concertations entre tous les acteurs sur les sujets encore en réflexion.

Remerciements

Nous tenons à remercier tout particulièrement notre pilote, Henri Serres, pour son soutien, sa relecture, les orientations et les conseils qu'il nous a prodigués.

Nous remercions également Alexis de Beauregard (Axa P&C) et Yves Verhoeven (ANSSI) pour leur soutien et l'accès privilégié à leurs ressources.

Nous avons eu la chance de rencontrer de très nombreux acteurs, dans les entreprises, au sein de l'État ou d'institutions. Nous les remercions très chaleureusement de l'accueil qu'ils nous ont réservé et espérons que ce mémoire contribuera modestement à faire progresser les débats.

ACTEURS PUBLICS

T. Auran, Chef du service des contrôles spécialisés sur place, ACPR
L. Bornia, Adjoint au chef du Bureau Assur 2, DG Trésor
D. Crochemore, Chef du bureau maîtrise des risques et règlementation, ANSSI
F. Ellis, Contrôleur des assurances, ACPR
L. Guerin, Chef du bureau Assur 1, DG Trésor
P. Laurier, Chercheur, IRT SystemX
J. Notin, Chef du projet Acyma, ANSSI
S. Oger, Chargée de mission, ANSSI
P. Picard, Professeur d'économie, École Polytechnique
J. Ricard, Adjoint au chef du bureau Assur 1, DG Trésor
Y. Verhoeven, Sous-directeur relations extérieures et coordination, ANSSI
P. Wolf, Directeur du projet EIC, IRT SystemX
L. Wolfrom, Policy Analyst, OCDE

ACTEURS PRIVÉS

B. Alleman, Directeur des assurances, Groupe EDF
A. Arnaud, Responsable sécurité informatique Groupe, TF1
F. Beaume, Director Risk and Insurance, Bureau Veritas
M.-E. Bellot, Responsable recherche et développement MidCorp, Allianz France
F.-C. Besson, Chief Underwriting Officer, Total
A. Bouillé, DSSI, Caisse des Dépôts, Président, CESIN
B. Bouquot, VP Risk Manager, Thales, Présidente, AMRAE
F. Bourdoncle, Président, FbCIE
M. Camillo, Vice President, AIG
E. Constance, Cyber Senior Vice President, Paragon Brokers
P. Cotelle, Head of Insurance Risk Management, Airbus Defence and Space
G. Courtois, Avocat associé, De Gaulle Fleurance & Associés
T. Crespe, Senior broker - Cyber practice leader, Aon
A. de Beauregard, Head of Business Development Retail P&C, Axa Global P&C
H. de l'Estoile, Directeur exécutif, AMRAE
C. Delcamp, Directeur adjoint assurances de biens et responsabilité, FFA
V. Denouail, IT manager, Total Marketing & Services

R. Divol, EVP and GM – Website Security, Symantec

D. Février, Responsable d'études actuarielles, RM lignes vie, Axa France

P. Gache, Chef du contrôle interne des SI, Groupe Orange

P. Gaillard, Directeur risques techniques et cyber, Axa France

J.-P. Gaulier, CISO, Groupe Orange

F. Gimenez, DSI, Groupe Total

C. Goujon, Chef de service juridique, TF1

L. Grynbaum, Of Counsel, De Gaulle Fleurance & Associés

E. Gurfinkiel, Juriste digital, TF1

S. Héon, Deputy Chief Underwriting Officer – Cyber Solutions, Scor

L. Heslault, Director, Security Strategist, Symantec EMEA

A. Ia, Specialty Lines Non-Marine VP - Cyber risks officer, CCR RE

T. Jaumain, Directeur des assurances, Arkema

S. Jean, Directeur du Hub Midcorp, Allianz France

R. Jezequel, Expert technique, CNPP

A. Kashyap, Director of Product Management, Symantec

M. Kociemba, élève avocate

S. Kuntz, Responsable de la Gestion des Risques IARD et Risques opérationnels, Axa France

J.-C. Laroche, DSI, Enedis

V. Lemoues, VP Corporate Risk Management and Insurance, Total

J.-M. Letort, VP Cybersecurity Evaluation & Consulting, Thales

O. Ligneul, CTO & Group CISO, EDF

A. Magnan-Leroyer, directrice de la direction technique RC & lignes financières, AON France

P. Marie-Jeanne, CRO, Axa France

J. Marlot, Head of Product Marketing, Orange Cyberdefense

J. Matillon, Directeur général, Bureau Veritas certification

L. Mayet, Président, GM Consultant

J. Menissez, Pre-sales consultant – CISSP, Airbus Defence and Space

J. Merlot, Directeur des assurances, Groupe Orange

L. Midrier, Vice-président stratégie et innovation, Bureau Veritas

J.-L. Moliner, Directeur de la sécurité, Groupe Orange

A. Nardone, Expert associé – Responsable risques IT, GM Consultant

M. Ortiz, Directeur du développement, De Gaulle Fleurance & Associés

D. Parsoire, Chief Underwriting Officer – Cyber Solutions, Scor

P. Pouillot, Senior Underwriter – Digital Risks, MunichRe

P.-L. Refalo, Global Head of Cyber Security Strategic Consulting, CapGemini Sogeti

J.-P. Regin, Senior Consulting Manager, Thales ISS

G. Rousseau, Souscripteur groupe - manager souscription, EDF Assurances

G. Savornin, CEO, CNPP

C. Seguela, RSSI Marketing & Services, Groupe Total

B. Serra, VP-Senior Credit Officer – Insurance Europe, Moody's

E. Silvestre, Directeur adjoint - Responsable souscription risques financiers - Entreprises Commerciales et Institutions financières, Liberty

B. Suzan, CIS, Technical Authority, R&T coordination and Innovation – Public Affairs, Airbus Defence and Space

J.-J. Tourre, RSSI, Groupe Total

L. Vignancour, Cyber & Crime Practice Leader, Marsh

F. Willi, Cyber Risk Reinsurance Specialist, Swiss Re

L. Zicry, Cyber Risks Practice Leader, Gras Savoye WTW

Bibliographie

Seules les références directement citées sont détaillées ici :

[1] R. Barjavel, Ravage, 1943.

[2] M. Ulsch, Cyber Threat!: How to Manage the Growing Risk of Cyber Attacks, Wiley, September 2014.

[3] C. Biener, M. Eling et J. H. Wirfs, «Insurability of cyber risk: an empirical analysis» University of St. Gallen, janvier 2015, http://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/wps/wp151.pdf

[4] R. Böhme et G. Schwartz, «Modeling Cyber-Insurance: Towards a Unifying Framework» *Workshop on the Economics of Information Security, Harvard,* n°151, mai 2010, http://www1.inf.tu-dresden.de/~rb21/publications/BS2010_Modeling_Cyber-Insurance_WEIS.pdf

[5] R. Pal et L. Golubchik, «On Economic Perspectives of Internet Security: The Problem of Designing Optimal Cyber-Insurance Contracts» University of Southern California, 2010, https://pdfs.semanticscholar.org/1e09/23b45edf7bb02c62cfa2c0c983db7b0f1055.pdf

[6] OCDE, Cyber Insurance: the market and available coverage, 2017 (diffusion restreinte OCDE).

[7] Cambridge Centre for Risk Studies - Risk Management Solutions, Inc., «Cyber Exposure Data Schema v1.0» 2016, http://cambridgeriskframework.com/getdocument/38

[8] CIGREF, «Le cyber risque dans la gouvernance de l'entreprise» octobre 2016, http://www.cigref.fr/wp/wp-content/uploads/2016/10/CIGREF-Cyber-risque-Gouvernance-2016.pdf

[9] World Economic Forum, «Advancing Cyber Resilience, Principles and Tools for Boards» janvier 2017, http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf

[10] PRA, «Consultation Paper CP39/16 : Cyber insurance underwriting risk» novembre 2016, http://www.bankofengland.co.uk/pra/Documents/publications/cp/2016/cp3916.pdf

[11] PRA, «Lettre aux souscripteurs de risques cyber» novembre 2016, http://www.bankofengland.co.uk/pra/Documents/about/letter141116.pdf

[12] ANSSI, «Guide d'hygiène informatique» janvier 2017, https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf

[13] HM Government, «Cyber Essentials Scheme, Requirements for basic technical protection from cyber attacks» juin 2014, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317481/Cyber_Essentials_Requirements.pdf

[14] C. Bertholet et L. Létourneau, Ubérisons l'État ! Avant que d'autres ne s'en chargent, Armand Colin, mars 2017.

[15] AIG, «Assurance Cyber : analyse des principales tendances» novembre 2016, https://www.aigassurance.fr/content/dam/aig/emea/france/documents/publications/guides-rapports/rapport-cyber-claims.pdf

[16] McAfee, «Tilting the Playing Field: How Misaligned Incentives Work Against Cybersecurity» mars 2017, https://www.mcafee.com/us/resources/reports/rp-misaligned-tilting-playing-field.pdf

[17] IRT SystemX, «La maîtrise du risque cyber sur l'ensemble de la chaîne de sa valeur et son transfert vers l'assurance» août 2016, http://www.irt-systemx.fr/v2/wp-content/uploads/2016/11/ISX-IC-EIC-transfert-risque-LIV-0401-v10_2016-10-25.pdf

Acronymes

ACPR	Agence de contrôle prudentiel et de résolution : régulateur français des banques et des assurances
ANSSI	Agence nationale de sécurité des systèmes d'information
APREF	Association des professionnels de la réassurance en France
CCR	Caisse centrale de réassurance
CIGREF	Club informatique des grandes entreprises françaises
CiSP	*Cyber security information sharing partnership* : initiative britannique de regroupement des données de sinistres cyber
(D)DoS	*(Distributed) denial of service* : Attaque en déni de service (distribué)
FFA	Fédération française de l'assurance
FGAOD	Fond de garantie des assurances obligatoires de dommages
FGTI	Fond de garantie des victimes des actes de terrorisme et d'autres infractions
GAFAM	Google, Amazon, Facebook, Apple et Microsoft représentant les géants américains du numérique
GAREAT	Gestion de l'assurance et de la réassurance des risques attentats et actes de terrorisme
GIP ACYMA	Groupement d'intérêt public pour le dispositif national d'assistance aux victimes d'actes de cybermalveillance
IoT	*Internet of things* : internet des objets
ISO	*Insurance services office* (US)
LMA	*Lloyd's market association* (UK)
OCDE	Organisation de coopération et de développement économiques
PME	Petites et moyennes entreprises
PRA	*Prudential regulation authority* : régulateur britannique des banques et des assurances
RGPD	Règlement général sur la protection des données
RSSI	Responsable de la sécurité des systèmes d'information
SI	Systèmes d'information
SPICE	*Scenario Planning for Identification of Cyber Exposure* : cadre d'analyse du risque cyber mis en place par Airbus Defence and Space