TOME I

JANVIER 2018

RAPPORT

ASSURER LE RISQUE CYBER

COMMISSION AD HOC CYBER RISK

le club des juristes

TOME I

ASSURER LE RISQUE CYBER

RAPPORT DU CLUB DES JURISTES

Commission ad hoc Cyber Risk

JANVIER 2018

Association déclarée - 4, rue de la Planche 75007 Paris
Tél. : 01 53 63 40 04

www.leclubdesjuristes.com

Retrouvez-nous sur :

Composition de la Commission

PRÉSIDENT :

Bernard Spitz, Président de la Fédération Française de l'Assurance (*FFA*)

SECRÉTAIRE GÉNÉRALE :

Valérie Lafarge-Sarkozy, Avocat associé, cabinet *Altana*

MEMBRES :

Nicolas Arpagian, Strategy & Public Affairs Director, *Orange*

Agathe Billiau-Lepage, Professeur à l'Université Panthéon-Assas, Paris II

Brigitte Bouquot, VP Insurance and Risk Manager, *Thales*,
Présidente de l'Association pour le management des risques et des assurances de l'entreprise (*AMRAE*)

Agnieszka Bruyère, Directeur Security Services, *IBM France*

Alice Chérif, Substitut du procureur au pôle Cybercriminalité,
Tribunal de grande instance de Paris

Philippe Cotelle, Head of Insurance Risk Management Cyberdefense,
Airbus Defence and Space,
Vice-Président de l'Association pour le management des risques et des assurances de l'entreprise (*AMRAE*)

Georgie Courtois, Avocat associé, *De Gaulle Fleurance & Associés*

Christophe Delcamp, Directeur adjoint des assurances de dommages et responsabilité, *FFA*

Emilie Dumérain, Déléguée juridique, *Syntec Numérique*

Philippe Gaillard, Directeur Dommage entreprises, Risques techniques et cyber, *Axa France*

Charles-Henry Madinier, Head of Marsh Risk Consulting France, *Marsh*

Alexandre Menais, Executive Vice President and Group Head of M&A, Strategy & Development, *Atos*

Séverine Oger, Chargée de mission auprès du sous-directeur relations extérieures et coordination, Agence nationale de la sécurité des systèmes d'information (*ANSSI*)

Martin Pailhes, Responsable de l'équipe juridique « Information Technology – Intellectual Property », *BNP Paribas*

Didier Parsoire, Chief Underwriting Officer Cyber Solutions, *SCOR*

Christian Poyau, Président de *Micropole*, Président de la Commission Transformation Numérique du *Medef*

Elisabeth Rolin, Conseillère juridique auprès du directeur général de l'Agence nationale de la sécurité des systèmes d'information (*ANSSI*)

Sylvie Sanchis, Chef de la brigade d'enquête sur les fraudes aux technologies de l'information (*BEFTI*), Direction de la police judiciaire de la Préfecture de Paris

Cécile Vignial, Senior consultant auprès de la Direction des Affaires Financières et d'Entreprise de l'*OCDE*

François Weil, Conseiller d'Etat

Leigh Wolfrom, Policy analyst – Directorate for Financial and Enterprise Affairs, *OCDE*

ONT CONTRIBUÉ À LA RÉDACTION DE CE CAHIER :

Cécile Vignial, Senior consultant auprès de la Direction des Affaires Financières et d'Entreprise de l'*OCDE*

Christophe Delcamp, Directeur adjoint des assurances de dommages et responsabilité, *FFA*

Nicolas Arpagian, Strategy & Public Affairs Director, *Orange*

Mariette Bormann, Directrice adjointe Conformité, *FFA*

Philippe Cotelle, Head of Insurance Risk Management Cyberdefense, *Airbus Defence and Space*,
Vice-Président de l'Association pour le management des risques et des assurances de l'entreprise (*AMRAE*),

David Crochemore, Chef de division méthode de management de la sécurité numérique, Agence nationale de la sécurité des systèmes d'information (*ANSSI*)

Laetitia Daage, Avocat, cabinet *Altana*

Philippe Gaillard, Directeur Dommage entreprises, Risques techniques et cyber, *Axa France*

Carole Gintz, Associate Managing Director, *Moody's Investors Service*

Célia Hamouda, Avocat, cabinet *Altana*

Olivier Hassid, Directeur, *PwC*

Sébastien Heon, Deputy Chief Underwriting Officer Cyber Solutions, *SCOR*

Marine Kociemba, Chargée d'études, *FFA*

Valérie Lafarge-Sarkozy, Avocat associé, cabinet *Altana*

Charles-Henry Madinier, Head of Marsh Risk Consulting France, *Marsh*

Jérôme Notin, Directeur général, Groupement d'Intérêt Public Action contre la cybermalveillance (*GIP ACYMA*)

Jean-Guy de Ruffray, Avocat associé, cabinet *Altana*

Benjamin Serra, Vice President – Senior Credit Officer, *Moody's Investors Service*

Emmanuel Silvestre, Senior Vice President Risques financiers, *Liberty Mutual*

Stéphane Spalacci, Responsable technique, *GAREAT*

Luc Vignancour, Cyber & Crime Practice Leader, *Marsh*

Leigh Wolfrom, Policy analyst – Directorate for Financial and Enterprise Affairs, *OCDE*

SECRÉTAIRE DE LA COMMISSION :

Bérénice Hahn de Bykhovetz, Doctorante à l'Université Panthéon-Assas, Paris II

CAHIER 1
Assurer le risque cyber

Des caravelles de Christophe Colomb à l'invention du moteur à explosion, de l'imprimerie aux nanosciences, le progrès technique a toujours généré de nouveaux risques. Cela n'a jamais été aussi vrai qu'avec les cyber-technologies. Il est désormais facile et peu coûteux d'accéder à des outils de piratage. Dans le même temps, la marche inexorable de la numérisation des processus de production multiplie les aubaines offertes aux délinquants. Ajoutons le facteur humain, qui introduit inévitablement des failles partout où l'on n'a pas, en amont, pensé des dispositifs protecteurs mais coûteux. La question du cybercrime n'est plus de savoir « si » mais « quand » il surviendra.

Les exemples parlent d'eux-mêmes. Le 7 septembre 2017, la société Equifax, l'une des plus importantes agences de crédit américaines, qui collecte et analyse les données personnelles de consommateurs sollicitant un prêt, a annoncé que son système informatique avait été piraté. En jeu, la fuite potentielle des données sensibles de pas moins de 143 millions d'Américains : noms, adresses, numéros de cartes de crédit ou de Sécurité sociale. Même chose pour 57 millions d'utilisateurs d'Uber.

En Europe, toujours en 2017, les hôpitaux britanniques, le fournisseur de télécoms espagnol Telefónica, Saint Gobain, le ministère russe de l'Intérieur ou la Deutsche Bahn, parmi beaucoup d'autres, ont été ciblés par les logiciels de ransomware « WannaCry » et « Petya ».

Démonstration est ainsi faite que nul n'est plus à l'abri.

Ces dangers sont loin d'être anecdotiques. Lloyd's of London a présenté le scénario d'attentat de grande ampleur qu'elle envisage le plus probable dans sa dernière étude sur les cyber-risques : l'attaque d'un prestataire de *cloud*. Lloyd's en estime les pertes dans une fourchette allant de 15 à 121 milliards d'USD, pour une moyenne évaluée à 53 milliards d'USD.

Face à ces enjeux, nos sociétés doivent se mobiliser à tous les niveaux : individus, professionnels et entreprises. En particulier les petites entreprises, qui, souvent, n'ont eu ni le temps, ni l'expérience organisationnelle, ni les moyens de se construire une politique de cyberdéfense cohérente. Attention danger pour celles qui se sont rassurées à tort, en pensant que les pirates ne s'attaqueraient qu'aux très gros.

Nos économies disposent d'un solide arsenal pour se protéger. Les professionnels savent déjà concevoir des solutions pour sécuriser la vie numérique des entreprises : il s'agit de fait pour eux de formidables occasions de développement et d'excellence. Le marché français de la cybersécurité a ainsi connu une croissance supérieure à 10 % en 2016, et ce n'est, pour le pire comme pour le meilleur, qu'un début. Mais ces entreprises restent encore à ce jour trop éclatées, de petite taille et dépendantes d'un financement encore trop faible, notamment de la part des acteurs privés.

Au premier rang des acteurs économiques, les assureurs et les réassureurs participent activement à l'évolution des économies numériques, même si l'Europe et la France affichent encore un retard certain.

Les chiffres parlent d'eux-mêmes : aujourd'hui, le marché mondial de l'assurance cyber est estimé entre 3 et 3,5 milliards d'USD. Le marché américain capte 85 à 90 % de ces primes. L'Europe, elle, ne représente encore que 5 à 9 % de ce marché, soit un montant maximum de 255 millions d'euros (300 millions de dollars) de primes, sur lesquels la France ne représente que 40 millions d'euros. Il y a de toute évidence un immense décalage entre pays développés quant à la perception du risque et à l'investissement assurantiel consenti pour s'en protéger.

Les pouvoirs publics français comme européens se sont saisis de la question. Ils ont lancé les fondements d'une nouvelle réglementation au sein de l'Union, dont la transposition est en cours. Ce premier pas est essentiel ; il n'est pas suffisant. L'existence d'un cadre juridique doit être accompagnée d'une vigilance de tous les acteurs économiques et du soutien durable des pouvoirs publics au développement d'une filière française et européenne de la cyber-protection.

Devant cette menace bien réelle, le Club des juristes, avec le concours de l'ensemble des parties concernées, a souhaité apporter sa contribution à une approche qui respecte toute la complexité de l'ensemble de ces dimensions économique, juridique et assurantielle.

Au terme de ses réflexions, le groupe, qu'on m'a fait l'honneur de présider, a dégagé, au-delà de l'état des lieux, un ensemble cohérent de recommandations. Dans un premier cahier on découvrira un éventail de solutions qui favoriseraient l'émergence d'une véritable assurance cyber. Le lecteur trouvera en fin de document nos dix préconisations pour une approche globale et efficace du problème. Deux autres cahiers suivront, examinant notamment la dimension juridique puis les conditions de prévention de ce nouveau cyber-risque, qu'il va falloir nous habituer désormais à comprendre, à combattre et à gérer.

Comme le disait le Général MacArthur : « Toutes les batailles perdues se résument en deux mots : trop tard. » C'est bien une bataille qui s'engage à l'aube du XXI^{ème} siècle. Puissions-nous nous donner toutes les chances de la gagner.

Bernard Spitz
Président de la Fédération Française de l'Assurance

Table des matières

À l'aube du développement des transports et territoires intelligents, des industries 4.0, de la réalité virtuelle, du traitement généralisé des données personnelles ou de l'Internet des objets, nous n'avons encore vu que les prémices de la transformation numérique. Elle bouleverse nos habitudes de communication et de consommation, ainsi que notre rapport à la santé, à l'énergie, à l'État ou à l'éducation, se glisse dans nos habitats et dans les fils de nos vêtements, se porte à notre poignet, fait battre les pacemakers, etc. Elle révolutionne les entreprises dans leur processus de production et de services, dans leurs relations à leurs clients, et dans leurs interconnexions à leur chaîne de valeur. Aujourd'hui, c'est un levier de croissance, d'innovation et de compétitivité essentiel pour les acteurs économiques.

Les risques sont à la mesure des enjeux ; parmi eux, le risque d'occurrence d'un incident cyber par lequel l'ensemble des bénéfices économiques et sociaux liés à la transformation numérique peut être compromis[1]. Une attaque cyber ou une erreur non intentionnelle de manipulation de données peut compromettre la confidentialité, l'intégrité et l'accessibilité de données et de systèmes d'information, se solder par de lourdes pertes financières, et menacer jusqu'à la survie d'une entreprise ou le fonctionnement et la sécurité d'un État.

En 2017, l'attaque « WannaCry » mi-mai, suivie de « NotPetya », détectée le 27 juin, et le piratage révélé le 25 septembre[2] de l'intégralité des courriels échangés entre les salariés du cabinet d'audit et de conseil Deloitte et ses clients pendant probablement six mois (les pirates auraient eu accès à cinq millions de messages) ont rappelé les menaces que le risque cyber fait peser sur l'économie et la société. Face à cette multiplication des incidents cyber, les agents économiques disposent de deux outils principaux et complémentaires : la prévention, qui sera le thème d'un autre cahier de ce groupe, et le transfert de risque par le biais de l'assurance pour les cas où les efforts de prévention ne suffisent pas à se prémunir contre un incident cyber.

(1) Voir OECD, *Supporting an effective cyber insurance market*, OECD report for the G7 Presidency, May 2017

(2) The guardian, *Deloitte hit by cyber-attack revealing clients' secret emails*, Sept. 2017, [https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails].

Le marché de l'assurance cyber contribue à réduire l'impact financier supporté par les acteurs économiques après une attaque grâce à une offre de couvertures et de services qui s'étoffe progressivement. Il contribue également à la prise de conscience de l'exposition au risque cyber, au partage d'expertise en gestion de ces risques, à l'encouragement des investissements en réduction des risques et à l'amélioration de la réponse aux incidents cyber[3].

En France, et plus largement en Europe, le marché de l'assurance cyber demeure toutefois embryonnaire, particulièrement sur le segment des TPE/PME. Or, les PME comptent pour 60 % des attaques recensées contre des entreprises en France[4].

Il faut aujourd'hui s'adapter à ce nouvel environnement juridique et économique particulièrement favorable pour améliorer les conditions du transfert du risque cyber. En optimisant leur protection financière en plus de leur sécurité numérique, les acteurs économiques renforceront la résilience de l'économie nationale et européenne face à un risque contre lequel nul ne peut se prétendre immunisé.

(3) OECD, *Enhancing the Role of Insurance in Cyber Risk Management*, 2017.
(4) Ministère de l'Intérieur, *État de la menace liée au numérique en 2017*, janvier 2017

PARTIE 1
L'assurance cyber en Europe : un marché en devenir

Des produits dédiés à la couverture du risque cyber ont été développés depuis près de vingt ans aux États-Unis, et depuis moins de dix ans en France. L'Europe représente à l'heure actuelle moins de 10 % du marché global de l'assurance cyber, qui semble lui-même très loin d'être à la mesure des risques encourus.

Pourquoi ce marché demeure-t-il à ce jour si étroit, en Europe, et notamment en France, et comment peut-on le rendre plus efficace pour les entreprises et autres acteurs économiques en quête de couverture contre les cyber-risques ?

I. Les spécificités du risque cyber

L'identification des spécificités du risque cyber au regard des critères d'assurabilité traditionnels[5] offre des éléments de réponse à ces questions.

Les critères d'assurabilité d'un risque sont traditionnellement classés en trois catégories[6] :

- actuariels (occurrence aléatoire / relative absence de corrélation entre les risques ; perte maximale qui peut être évaluée et couverte, et perte moyenne par événement modérées ; exposition au risque

(5) Ce chapitre se réfère notamment aux conclusions de l'une des rares recherches disponibles sur l'assurabilité des risques cyber : Biener, Christian, Eling, Martin, Wirfs, Jan H., *Insurability of cyber risk: an empirical analysis,* 2015.
(6) Berliner, *Limits of insurability,* 1982.

suffisante pour établir une base de données statistique ; aléa moral et sélection adverse limités) ;

- de marché (prime jugée abordable par les prospects au regard de la couverture offerte) ;
- sociétaux et réglementaires (restrictions légales à la couverture de certains risques notamment).

À l'heure actuelle, les risques cyber présentent un certain nombre de caractéristiques qui les placent à la frontière de l'assurabilité au regard de plusieurs de ces critères.

A. Des pertes qui pourraient s'alourdir considérablement dans le futur

Pour qu'un risque soit assurable, il faut que les pertes anticipées soient inférieures à la capacité disponible des assureurs pour les couvrir. L'évaluation de la perte moyenne, de la perte maximale et de la fréquence des pertes permet aux assureurs de calculer s'ils peuvent couvrir un risque sans mettre leur solvabilité en danger, pour une prime que les assurés potentiels pourront trouver abordable.

L'estimation du coût des incidents cyber est complexe. À titre d'exemple, le tableau suivant présente les résultats d'une collecte de données sur des pertes liées à des incidents cyber ayant touché des entreprises aux États-Unis pendant une période de dix ans.

Focus – Estimation du coût moyen, médian et maximal d'incidents cyber, 2005-2014*

Type d'événement	*N*	Coût moyen	Coût médian	Coût max.
Total (en millions de dollars)	921	7,84	0,25	750

** Les données mentionnées se réfèrent à un échantillon d'incidents étalés sur la période 2005-2014. Ils ne portent que sur des incidents qui ont fait l'objet d'estimations de coûts.*
Source : Romanosky, « Examining the costs and causes of cyber incidents », Journal of Cybersecurity, August 2016.

Le coût *global* maximal des incidents cyber est demeuré jusqu'à présent très inférieur à celui d'autres grands risques et de nombreuses catastrophes naturelles en particulier : le coût global de l'ouragan Katrina de 2005, par exemple, a été estimé à plus de 80 Mds d'USD 2016, dont environ 40 Mds étaient assurés ; celui d'autres catastrophes comme les attentats du 11 septembre 2001 a été estimé à 25 Mds d'USD 2016[7]. S'il est encore trop tôt pour mesurer l'impact global des attaques WannaCry et NotPetya, l'ampleur des pertes résultant d'autres incidents cyber passés (comme l'attaque d'Epsilon, qui lui a coûté quatre milliards d'USD, ou celle de Sony PlayStation – 171 millions d'USD) n'invite pas à conclure à l'insassurabilité des risques cyber.

Au-delà de l'augmentation progressive du coût des conséquences dommageables des incidents cyber ainsi que de leur fréquence, c'est surtout l'incertitude liée aux pertes potentielles futures résultant de méga-attaques ou de séries d'attaques de plus faible ampleur mais simultanées qui pose de nouveaux défis aux assureurs.

Les assureurs devront également faire face, à partir de 2018, à l'accroissement du coût des incidents cyber du fait des nouvelles obligations liées au développement du cadre réglementaire, et notamment à l'élargissement des obligations de notification à la charge de l'entreprise. L'anticipation de ces nouveaux coûts devrait accélérer la pénétration de l'assurance cyber.

Des scénarios récents présentent des pertes engendrées par un incident cyber majeur, prenant par exemple pour cible des infrastructures critiques qui ont par nature une grande capacité de diffusion, ou une

(7) Swiss Re Institute, *Catastrophe naturelle en 2016 : une année de dommages tous azimuts*, Sigma, no 2, fév. 2017.

série d'incidents (scénario de cyber-hurricane) qui pourrait atteindre des niveaux jamais atteints précédemment et mettre en danger la solvabilité d'un ou de plusieurs assureurs.

Au Royaume-Uni, par exemple, l'exposition de l'infrastructure des marchés financiers au risque cyber est une préoccupation majeure[8]. Un incident cyber de grande ampleur les affectant aurait un impact sur l'économie nationale et mondiale, dont le coût serait considérable.

Un assureur[9] a de même établi un parallèle entre la débâcle globale qui suivrait un incident cyber majeur, par exemple chez un grand acteur du *cloud*, dont les répercussions en cascade sur l'économie réelle (fournisseurs d'eau et d'énergie, appareils médicaux, réseaux bancaires ou de transports, etc.) seraient immédiates, et la faillite de Lehman Brothers et ses conséquences en cascade en septembre 2008. Le scénario d'attaque de grande ampleur présenté comme le plus probable dans la dernière étude du Lloyd's sur les risques cyber est également celui de l'attaque d'un prestataire de cloud. Selon le Lloyd's, les pertes pourraient se situer dans une fourchette allant de 15 à 121 Mds d'USD 2016, avec une moyenne évaluée à 53 Mds[10]. Ces chiffres sont comparables à ceux des plus grandes catastrophes naturelles cités précédemment[11].

Plusieurs observateurs en concluent que le risque cyber est actuellement le risque le plus important et le plus systémique.

Au regard de l'ampleur de certains événements cyber qui engendreraient de considérables cumuls de dommages, certains acteurs majeurs affirment que le risque dépasse la capacité d'absorption du marché[12] et que « certains cyber-risques, notamment ceux liés à des événements

(8) Voir par exemple Bank of England (2014), *The Bank of England's supervision of financial market infrastructures,* p. 10, qui présente les quatre piliers du programme établi pour augmenter la résilience du secteur financier face aux risques cyber.
(9) Zurich, *Beyond Data Breaches : Global Interconnection of Cyber Risk,* 2014.
(10) Lloyd's, *Counting the Costs, Cyber Exposure Decoded,* Emerging Risk Report 2017, juil. 2017, p. 30.
(11) Il est toutefois rappelé que seul un segment de ces pertes (les pertes assurées) serait à la charge des assureurs. En prenant en compte des estimations relatives à la pénétration, aux limites et aux rétentions, le Lloyd's a évalué à 4,60 Mds d'USD les pertes assurées pour un scénario de pertes globales de 53,05 Mds d'USD.
(12) Financial Times *Cyber risks too big to cover, says Lloyd's insurer*, citant Stephen Catlin., 5 fév. 2015, [https://www.ft.com/content/94243f5a-ad38-11e4-bfcf-00144feab7de?mhq5j=e3].

dommageables extrêmes ou catastrophiques, tels que la perturbation d'infrastructures ou de réseaux critiques, pourraient demeurer inassurables[13]».

B. Des risques potentiellement fortement corrélés

L'assurance repose notamment sur la mutualisation des risques. L'assureur peut généralement prévoir la perte moyenne (et donc la prime) par assuré en appliquant la loi des grands nombres selon laquelle l'indemnité moyenne par assuré, si elle est aléatoire, n'en est pas moins quasiment constante, lorsque les dommages sont distribués de manière identique et indépendante.

Or, dans le cas des cyber-risques, l'application de la loi des grands nombres est entravée par l'interdépendance des systèmes informatiques et des acteurs économiques, qui multiplie les probabilités de propagation de certains types d'incidents cyber. Ainsi, un virus informatique peut se propager en s'autorépliquant dans un programme légitime et passer d'un ordinateur à un autre en infectant les systèmes qu'il rencontre. De plus (à l'inverse des virus biologiques qui se transmettent d'un individu à l'autre), les virus informatiques peuvent se transmettre « à partir d'un seul nœud à *n* ordinateurs de x entreprises[14] ». Ils peuvent ainsi infecter quasi instantanément des dizaines de milliers d'ordinateurs, comme récemment le logiciel malveillant NotPetya, qui s'est servi de la procédure de mise à jour d'un logiciel de comptabilité ukrainien pour infecter diverses cibles en Ukraine, dont l'aéroport de Kiev ainsi que le système de surveillance des radiations de la centrale nucléaire de Tchernobyl, avant de contaminer la Russie, le Royaume-Uni, la Norvège, les Pays-Bas ou la France, le 27 juin 2017, seulement cinq heures après la première détection du virus.

La suprématie de certains systèmes d'exploitation (comme Microsoft Windows), qui rend de nombreux ordinateurs/systèmes vulnérables au même incident[15], accroît encore la corrélation des risques. L'impact de

(13) Swiss Re, Cyber : *getting to grips with a complex risk*, Sigma 1/2017, p. 38.
(14) A. JAGHADAM, « Les conditions d'assurabilité des cyber-risques », Revue *Risque*, no 77, 2009.
(15) D. GEER, *Cyber Insecurity : The Cost of Monopoly*, Computer and Comm. Industry Assoc., 2003, [http://www.ccianet. org/papers/cyberinsecurity.pdf.].

WannaCry, qui exploitait une faille des systèmes d'exploitation Microsoft Windows antérieurs à Windows 10, dont les mises à jour de sécurité n'avaient pas été effectuées, l'a encore récemment illustré.

Cette corrélation entre de nombreux risques cyber pose un double défi aux assureurs. D'une part, elle complique leur stratégie de diversification de leur portefeuille de risques, garante de leur solvabilité, elle entraîne des risques de cumuls. La diversification géographique des risques souscrits est par exemple inopérante puisque les incidents cyber peuvent être transfrontières. Par opposition aux risques de catastrophes naturelles, dont les conséquences sont généralement confinées dans une seule région, de nombreux incidents cyber peuvent se développer instantanément dans un large périmètre national ou international. Un pays entier peut être affecté, comme l'Estonie, qui a subi, en 2007, la première cyberattaque recensée contre un État[16]. D'autres types d'attaques ont d'emblée une portée mondiale, comme WannaCry et NotPetya. « Le monde entier devient une zone de cumul[17]. » Les incidents cyber entraînent également un cumul de lignes d'assurances affectées (dommage, pertes d'exploitation, accident du travail, RC, etc.).

D'autre part, la corrélation entre un grand nombre de risques rend la quantification du risque et la définition de la prime d'assurance beaucoup plus complexes. En effet, le niveau de risque cyber d'une entreprise ne dépend pas uniquement de ses propres efforts de prévention. Un maillon faible dans sa chaîne de valeur peut contaminer tout son écosystème (sous-traitants, contreparties, chaînes d'approvisionnement, clients, etc.). La notion de « sécurité interdépendante[18] », qui a été utilisée pour caractériser le risque de terrorisme, est également très pertinente pour le cyber-risque.

Comme le rappelle une récente étude de Swiss Re[19], le degré de dépendance dépend du type de menace cyber considérée.

(16) Une attaque coordonnée à partir de 60 pays différents a saturé les sites de son Parlement, des ministères, des banques et des médias, causant un déni de service prolongé.
(17) A. JAGHADAM, « Les conditions d'assurabilité des cyber-risques », Revue Risque, no 77, 2009, note 5.
(18) H. KUNREUTHER, E. MICHEL-KERJAN, *Insurability of (mega) terrorism risk : challenges and perspectives in OECD* (2005), Terrorism Risk Insurance in OECD Countries, 2005.
(19) Swiss Re, Cyber : *getting to grips with a complex risk*, in Sigma 1/2017 p. 19.

Focus – Pertes probables au sein et à l'extérieur de l'entreprise en fonction du type d'incident cyber*

	Dégâts au sein de l'entreprise	**Dégâts à l'extérieur de l'entreprise**
Défaillance d'un ordinateur personnel en raison d'un problème de matériel	Limités	Limités
Personne interne à la société qui abuse de ses droits d'accès	Pourrait affecter la quasi-totalité des ordinateurs du réseau interne et provoquer une perturbation significative au sein de sa société	Probablement limités
Attaques impliquant une interaction avec les utilisateurs, telles que le phishing (hameçonnage) ou le spyware (logiciel espion) / malware (logiciel malveillant)	Possibilité de perturbation significative	Peuvent entraîner des vulnérabilités corrélées entre firmes si quelques employés dans un grand nombre de sociétés différentes sont ciblés
Autres types d'attaques : logiciels malveillants, tels que les vers, les virus et les chevaux de Troie	Dégâts corrélés	Dégâts corrélés

* Source : d'après Swiss Re (2017), Sigma 1/2017 – *cyber : getting to grips with a complex risk*, p. 19

Ces interdépendances entre appareils/systèmes informatiques augmentent de façon exponentielle dans nos sociétés de plus en plus numériques : l'extension du périmètre de la transformation numérique des organisations, la corrélation entre des millions d'utilisateurs hyperconnectés dans l'architecture d'Internet, l'utilisation généralisée de logiciels susceptibles de se révéler vulnérables, l'explosion du nombre de dispositifs connectés et le recours au *cloud* sont autant de catalyseurs majeurs de la corrélation des risques. Des risques encore isolés il y a quelques années dans le portefeuille d'un assureur – ceux d'entreprises clientes dans différentes régions du monde ou différents secteurs d'activité, dont les systèmes informatiques dépendent de différents opérateurs, etc. – peuvent, par exemple, se retrouver instantanément corrélés par leur décision d'abriter leurs données au sein du même *cloud*.

Si elle n'empêche pas la souscription d'assurance et peut être contournée par divers moyens, dont la réassurance, la corrélation des risques cyber demeure donc une source d'incertitude et de cumuls et rend indéniablement plus complexe la définition d'une offre d'assurance cyber pertinente.

C. Une absence de base de données statistique fiable sur la cyber-sinistralité

Pour être assurables, les pertes associées à un risque donné doivent être estimées et modélisées grâce à l'analyse de séries historiques d'événements passés.

Dans le cas du risque cyber, on ne dispose toutefois que de peu de recul sur la fréquence et la sévérité des incidents cyber : le risque lui-même étant récent, les calculs actuariels se fondent sur des séries historiques étroites.

De surcroît, les bases de données actuarielles sur les incidents passés sont tronquées. Pour préserver leur réputation et éviter les poursuites en cas de violations de données personnelles, de nombreux acteurs économiques choisissent de ne pas révéler publiquement les incidents cyber dont ils ont été victimes, ou de taire le montant des pertes subies.

D'autres ignorent qu'ils ont été victimes d'attaques, de plus en plus difficiles à détecter. Certaines attaques récentes n'ont en effet été identifiées que plus d'un an après l'intrusion.

En outre, la plupart des données disponibles sont publiées par des entreprises liées au conseil ou à l'édition de solutions en cybersécurité ou au transfert de risque, ce qui induit deux biais potentiels : leur intérêt n'est pas de minimiser la menace et leurs données – qui reposent souvent principalement sur l'échantillon statistique constitué de leur clientèle – sont partielles.

Étroites et partiellement biaisées, les bases statistiques disponibles sur les incidents cyber pâtissent également de deux contraintes techniques.

D'une part, il n'existe pas de méthodologie standardisée pour inventorier de manière homogène les incidents cyber et leur impact à l'échelle nationale et internationale. Quels incidents cyber devraient être comptabilisés dans une base de données ? Faudrait-il établir un seuil en fonction de leur gravité, pour éviter que les autorités responsables de la collecte d'information soient noyées sous des flots de notifications d'incidents mineurs et sans réelles conséquences dommageables ? Comment un seuil de gravité devrait-il être défini ? L'absence de réponses partagées entraîne des biais dans la comparaison des statistiques publiées.

D'autre part, si les organismes privés qui publient des statistiques liées aux incidents cyber sont nombreux (prestataires informatiques, consultants, etc.), il n'existe pas à ce jour en France d'organisme, privé ou public, dont la mission est de collecter et d'anonymiser les incidents cyber à l'échelle nationale afin de produire des statistiques qui pourraient être partagées avec tous les acteurs du marché.

Cette absence de base de données fiable prive les assureurs d'un outil de travail essentiel pour modéliser les risques cyber et l'ensemble des acteurs économiques d'une source d'information qui contribuerait à une prise de conscience accrue du risque cyber.

D. Des pertes largement intangibles, difficiles à évaluer[20]

Le risque cyber génère souvent des dommages intangibles, très difficiles à évaluer, comme la dégradation de la réputation d'une marque à la suite d'une violation massive des données. La méfiance dans la capacité de l'entreprise à garantir ses propres données et les données de ses clients peut alors être forte et durable, et causer un réel préjudice à l'entreprise. Ce type de dommages est susceptible d'être considérable : la perte de valeur de la marque d'une entreprise victime d'une violation de données aux États-Unis en 2015 a été estimée à un montant moyen compris entre 184 et 330 millions d'USD selon le type de données compromises[21]. De plus, les attaques visant de grands groupes tels Sony, Target et Equifax montrent que, face à une attaque de grande ampleur, la valorisation boursière de l'entreprise peut également être affectée à court terme.

Ces impacts tendraient toutefois à diminuer à mesure que le nombre d'attaques cyber augmente. En effet, avec la banalisation de ce type d'incidents, les clients des entreprises cibles et leurs actionnaires tendent à les pénaliser moins, ou moins longtemps, et l'impact sur le prix des actions diminue[22].

(20) Cf. chapitre précédent.
(21) Ponemon Institute, *Reputational Impact of a Data Breach Study*, 2015.
(22) Artemis (2017), *Cyber risks and government pools. Too soon?, Artemis news articles*, 30 March, [www.artemis.bm/blog/2017/03/30/cyber-risks-and-government-pools-too-soon/].

L'exemple d'Equifax

Le 7 septembre dernier, la société Equifax, l'une des plus importantes agences de crédit américaines, qui collecte et analyse les données personnelles de consommateurs sollicitant un crédit, a annoncé avoir subi un piratage de son système informatique. L'incident a provoqué la potentielle fuite des données sensibles de l'ordre de 145 millions[23] de Nord-Américains (noms, adresses, numéros de cartes de crédit ou de Sécurité sociale…).

Le 7 septembre, le cours de l'action Equifax au New York Stock Exchange s'élevait à 142,7 USD.

Le 8 septembre, l'action cotait 123,23 USD, enregistrant une perte de 14 %.

Le 15 septembre, l'action cotait 92,92 USD, perdant en une semaine 35 % de sa valeur. À cette même date, Equifax a annoncé le licenciement du responsable de la sécurité et du directeur informatique. À compter de cette date, le cours de l'action a commencé à remonter.

Le 22 septembre, le Chief Executive Officer d'Equifax, Richard Smith, a démissionné.

(23) Estimation au 5 octobre 2017.

E. Une analyse du risque à assurer complexe, du fait de la technicité et de la sensibilité des informations échangées

La couverture de cyber-risques requiert des assureurs une expertise cyber pointue et une fine connaissance de l'entreprise cliente pour comprendre les menaces auxquelles elle doit faire face et appréhender l'ensemble de ses expositions et vulnérabilités cyber que lui présente le Risk manager ou la direction en charge du sujet.

Toutefois, les assurés sont souvent peu enclins à partager avec les assureurs et autres prestataires associés à la souscription du contrat l'ensemble des informations qui permettraient de quantifier précisément leur exposition au risque : ces données, qui concernent le cœur de leur activité et leur valeur (projets en cours, brevets, etc.), sont particulièrement stratégiques et confidentielles.

Aussi, les entreprises sont parfois réticentes à partager des informations relatives au niveau de résilience de leurs systèmes d'information, y compris les systèmes opérationnels, et notamment les conclusions de leurs tests d'attaques à « blanc » pour celles qui se soumettent à ce type d'exercice.

À ce stade de son développement, le marché de l'assurance cyber est donc soumis à une asymétrie d'information qui peut être très importante entre assureurs et assurés. Celle-ci peut empêcher le calcul d'une prime d'assurance adaptée aux spécificités du profil de l'assuré, et ainsi générer des phénomènes d'anti-sélection : les entreprises déjà victimes d'attaques, et celles qui s'estiment le plus à risque, sont plus enclines à s'assurer que les autres, déséquilibrant le portefeuille de risque des assureurs.

F. Un risque fortement dynamique

Environ 90 % des sinistres cyber déclarés « résultent d'une erreur humaine ou d'un comportement humain[24] ». L'imprévisibilité du comportement

(24) W.TOWER WATSON, *En matière de cybersécurité, les entreprises oublient le facteur humain*, 7 mars 2017, [https://www.willistowerswatson.com/fr-FR/press/2017/03/when-it-comes-to-cyber-risk-businesses-are-missing-the-human-touch].

humain, volontaire ou involontaire, dont dépendent l'occurrence et la sévérité de nombreux incidents cyber (probabilité de vol ou d'erreurs de manipulation de données, du choix de la cible en cas d'attaque, etc.), rend les risques cyber intrinsèquement plus versatiles et difficiles à prévoir et à modéliser que d'autres types d'événements.

En outre, comme pour le risque terroriste, le choix des cibles et des modalités d'attaques s'adapte continuellement à divers paramètres[25], comme le niveau de protection des cibles ou les capacités de gains (liées, par exemple, aux fluctuations des prix de revente des données volées sur le *dark web*), créant une « incertitude dynamique[26] ». Celle-ci complique l'anticipation des risques, par rapport aux catastrophes naturelles, dont la localisation n'est pas fonction de la vulnérabilité des sites.

Par ailleurs, le risque d'attaques cyber a connu en quelques années une profonde mutation du fait de la sophistication rapide du profil des cyberattaquants. Aux adolescents geeks en quête de défi ou de reconnaissance se sont ajoutées des bandes du crime organisé, professionnelles, parfois soutenues par des États dont les motivations sont financières (i.e extorsions), économiques (i.e. espionnage industriel) ou politiques (i.e. déstabilisation d'un État, représailles en réponse à son action diplomatique, influence dans un processus d'élections…). Parallèlement à cette professionnalisation des cyberattaquants, on observe une prolifération d'acteurs, qui, sans moyens ni expertise, profitent de l'offre accrue de solutions d'attaques clé en main à bas coût sur le marché noir[27]. Fortinet mettait ainsi récemment en garde contre le développement de solutions *ransomware-as-a-service*, démultipliant les risques de ce type d'attaques[28]. Si les traditionnels vols de données revendues sur le *dark web* sont toujours une source importante de dommages, le coût des rançongiciels (blocage d'accès à des données ou à un système dans l'attente

(25) Pour une infographie des types d'attaques par secteur, voir Lloyd's, en association avec KPMG et DAC Beachcroft (juin 2017), *Closing the gap – insuring your business against evolving cyber threats*, p. 18.
(26) Voir par exemple H. KUNREUTHER, E. MICHEL-KERJAN, *Insurability of (mega) terrorism risk : challenges and perspectives in OECD* (2005), Terrorism Risk Insurance in OECD Countries, 2005.
(27) Swiss Re (2017), Cyber, *comment venir à bout d'un risque complexe ?,* Sigma no 1/2017.
(28) J. ROMMEL, *Ransomware-as-a-Service : Rampant in the underground Black Market,* Fortinet, 16 fév. 2017, [https://blog.fortinet.com/2017/02/16/ransomware-as-a-service-rampant-in-the-underground-black-market]

du paiement d'une somme souvent libellée en bitcoins) aurait atteint un milliard d'USD en 2016[29]. Ces évolutions des attaques cyber doivent être comprises et anticipées par les assureurs.

Le risque cyber a également évolué au rythme des progrès technologiques des systèmes informatiques et électroniques toujours plus puissants, et de l'élargissement de périmètre de l'espace cyber. L'avènement des objets connectés et les progrès de l'intelligence artificielle ont ouvert une nouvelle ère d'opportunités, dont les cyberattaquants ont immédiatement tiré parti. Le 21 octobre 2016, l'accès à Amazon, Netflix, Twitter ou PayPal a été interrompu dans une partie des États-Unis à cause de l'attaque du producteur de cloud Dyn par le biais d'objets connectés (caméras de télésurveillance en réseau). Le recours à l'intelligence artificielle pour « créer des tweets personnalisés et inciter des cibles à cliquer sur des liens malveillants[30] » a également été récemment mis en évidence.

Enfin, comme pour le risque de terrorisme, l'action des États peut avoir un réel impact sur le niveau de risque cyber, ainsi que sur le choix des cibles. Les États peuvent aussi être eux-mêmes à l'origine d'attaques cyber. Leur ligne politique et diplomatique peut également faire l'objet de cyber-représailles. La dimension étatique des risques cyber introduit une incertitude supplémentaire dans le calibrage du risque.

Cette dynamique complique considérablement le travail de modélisation des risques par l'assureur. À l'instar des Risk managers et gestionnaires de risques dans les entreprises, et des fournisseurs de solutions de sécurité, les assureurs doivent se former continuellement et opérer une veille technologique constante sur les nouvelles vulnérabilités et formes d'attaques des systèmes. De ce fait, l'analyse des incidents passés n'a qu'une valeur prédictive limitée. La construction de scénarios prospectifs et disruptifs est donc particulièrement importante dans ce marché immature.

Les difficultés énumérées ci-dessus sont pour l'assureur autant de freins au développement du marché cyber. Toutefois, comme pour les risques de catastrophes naturelles, de terrorisme ou environnementaux, l'expérience

(29) Idem.
(30) Swiss Re (2017), *Cyber, comment venir à bout d'un risque complexe ?* Sigma no 1/2017, p. 7.

croissante des assureurs et le recours à la réassurance, notamment, leur permettront d'améliorer progressivement leur offre à destination des entreprises.

II. L'évolution de l'offre d'assurance cyber

Les conséquences dommageables consécutives à des faits générateurs cyber, accidentels ou malveillants ne sont que partiellement couvertes par les contrats traditionnels existants, qui n'ont pas été conçus pour une économie largement numérique comme celle que nous connaissons aujourd'hui. De nouveaux contrats dédiés spécifiquement aux risques cyber ont donc été progressivement développés pour couvrir les conséquences dommageables qui ne sont pas nécessairement prises en charge par les contrats traditionnels.

A. Un risque partiellement couvert par les contrats traditionnels

Avant que des contrats spécifiques ne se développent, de nombreuses conséquences dommageables d'un cyber-risque étaient déjà (et sont toujours, sauf exclusions spécifiques) couvertes par les contrats d'assurance traditionnels.

1. Les contrats de dommages aux biens

Les faits générateurs cyber, qu'ils soient d'origine malveillante ou issus d'erreurs humaines, peuvent engendrer des conséquences dommageables matérielles. Elles seront couvertes par le contrat dommages aux biens.

Avec ce contrat, les dommages physiques aux biens de l'assuré et les pertes d'exploitation consécutives seront couverts quel que soit le fait générateur cyber. A contrario, si le fait générateur cyber ne crée pas de dommage matériel, les pertes d'exploitation ne peuvent être couvertes par ce contrat.

Focus – Explosion d'un pipeline de BTC Turquie en août 2008

Les faits

En août 2008, une partie du pipeline de BTC a explosé en Turquie. Le fait générateur de cette explosion était une attaque cyber malveillante : les attaquants se sont introduits dans le système d'exploitation de la station de raffinage, en ont pris le contrôle et ont déréglé les calculs de pression et de débit, entraînant une explosion de la station de raffinage. Cette dernière a été hors d'usage pendant une durée de trois semaines[31]. L'exploitant a consécutivement subi d'importantes pertes financières.

Les éventuelles conséquences sur le contrat de dommages aux biens si cet incident cyber avait été assuré en France

Dans ce cas, les dommages matériels et les pertes d'exploitation en résultant auraient pu être pris en charge par les contrats de dommages de l'exploitant.

2. Les contrats de responsabilité civile

Par nature, les contrats de responsabilité civile couvrent les dommages corporels, matériels et immatériels causés aux tiers, quel que soit leur fait générateur. Ils couvrent également les frais de défense et de recours de l'assuré lorsque ce dernier est la victime. Par conséquent, les sinistres de responsabilité civile résultant d'un fait générateur cyber d'origine malveillante ou consécutifs à une erreur humaine seront couverts par ces contrats.

Par exemple, un responsable de traitement de données à caractère personnel mis en cause pour atteinte à la vie privée[32] à la suite d'une violation puis d'une divulgation de données à caractère personnel consécutive à un acte de malveillance ou à un accident pourra être couvert par son contrat de responsabilité civile.

(31) EURASIANET, *U.S. Intelligence : Russia Sabotaged BTC pipeline Ahead of 2008 Georgia War*, 10 déc. 2014, [http://www.eurasianet.org/node/71291].
(32) Code civil, art. 9.

Il en va de même pour une entreprise victime d'une cyberattaque qui la contraint à arrêter sa production et à suspendre ses livraisons. Par manque d'approvisionnement, ses propres clients peuvent également être amenés à arrêter leur production. Ils subissent alors un préjudice dont l'entreprise victime de l'attaque cyber pourra être tenue responsable. Ces préjudices pourront être couverts par le contrat de responsabilité civile de l'entreprise victime de la cyberattaque.

Focus – Vol de données chez Intercontinental Hôtels Group, décembre 2016

Les faits

Un virus informatique a contaminé les serveurs de 1 200 hôtels de la chaîne Intercontinental Hôtels Group, en décembre 2016. Les pirates ont pu ainsi avoir accès aux données relatives aux cartes de paiement des clients. Les clients concernés par ce vol de données en ont été informés par la société. Des frais ont été engagés à cet effet. Ce malware n'aurait été éradiqué qu'en mars 2017[33].

Les éventuelles conséquences sur le contrat d'assurance de responsabilité civile des hôteliers si cet incident cyber avait été assuré en France

- Les clients des hôtels concernés par le vol de données auraient pu engager la responsabilité du groupe hôtelier pour atteinte à la vie privée.
- Les organismes émetteurs de cartes bancaires (Visa, MasterCard…) ont dû résilier les cartes compromises et en émettre de nouvelles. Ils pourraient réclamer les frais ainsi engagés à la chaîne d'hôtels. Les dommages causés aux tiers auraient pu être pris en charge dans le cadre du contrat de responsabilité civile du groupe hôtelier sous réserve des exclusions spécifiques éventuellement prévues au contrat.

(33) *Le JDD,* « Comment les entreprises se défendent face aux cyberattaques », 25 avr. 2017, [http://www.lejdd.fr/economie/comment-les-entreprises-se-defendent-face-aux-cyberattaques-3310139].

3. Le contrat Responsabilité des dirigeants

Le contrat d'assurance Responsabilité des dirigeants couvre les frais de comparution, les frais de défense, ainsi que les conséquences pécuniaires encourues par tout dirigeant d'entreprise mis en cause à titre personnel et reconnu responsable envers sa société, ses actionnaires ou ses associés, ou encore tout tiers (autorités régulatrices, créanciers, salariés, fournisseurs…) en raison du non-respect des lois ou des règlements, de la violation des statuts sociaux, ou encore de toutes fautes de gestion allant, selon les types d'actions engagées à son encontre, de la faute séparable de ses fonctions à la simple inaction fautive.

À la suite d'un événement cyber, la responsabilité des dirigeants pourrait être retenue (pour non prise en compte du risque).

Les contrats d'assurance couvrant la responsabilité des dirigeants peuvent couvrir de tels faits générateurs.

4. Le contrat Fraude

Les contrats Fraude existent de longue date. Ils couvrent les actes frauduleux tels que le détournement de fonds, l'escroquerie, le faux ou l'usage de faux, la contrefaçon et le vol.

Les conséquences dommageables d'une fraude assistée par ordinateur sont couvertes par les contrats Fraude et non pas par les contrats cyber. À titre d'exemple, les faux ordres de virement par usurpation d'identité (fraude au président) restent du périmètre exclusif des contrats Fraude, même s'ils utilisent des nouvelles technologies (faux e-mails, usurpations d'identité numérique…).

Lorsque la fraude est facilitée par l'introduction d'un logiciel malveillant dans le système informatique, les conséquences dommageables de ce seul fait générateur pourront être couvertes soit par les contrats Fraude soit par les contrats cyber.

B. Le développement de contrats spécifiques

L'émergence de nouveaux risques liés à l'évolution des nouvelles technologies de l'information et de la communication et à l'accroissement de leurs usages a nécessité et nécessite encore la mise en place de cadres juridiques adaptés. Ainsi, en France, la loi informatique et libertés de 1978 consolidée[34] et celle de programmation militaire pour la période 2014-2019[35] ont introduit de nouvelles obligations pour les entreprises, dont l'exécution ou le non-respect induit de nouveaux frais qui ne sont pas pris en charge par les contrats traditionnels (ex. : obligation de notification, enquête administrative).

Ces nouveaux risques ont entraîné l'apparition d'un nouveau type de dommages, comme les atteintes aux données personnelles des tiers et de l'entreprise, ou les pertes d'exploitation consécutives, qui ne sont pas prises en charge par les contrats traditionnels.

Pour faire face à ces nouveaux risques, de nouveaux services ont été développés par les assureurs, de plus en plus nombreux à nouer, à cette fin, des partenariats avec des entreprises liées au conseil et/ou à l'édition de solutions en cybersécurité. Ces services peuvent être regroupés en quatre catégories :

- des analyses de risques ;
- les recherches de causes, ou « forensic » ;
- la gestion de crise ;
- la couverture des frais de monitoring bancaires.

Ces nouveaux besoins de garanties et de services ont conduit à la création d'un nouveau contrat : le contrat d'assurance cyber.

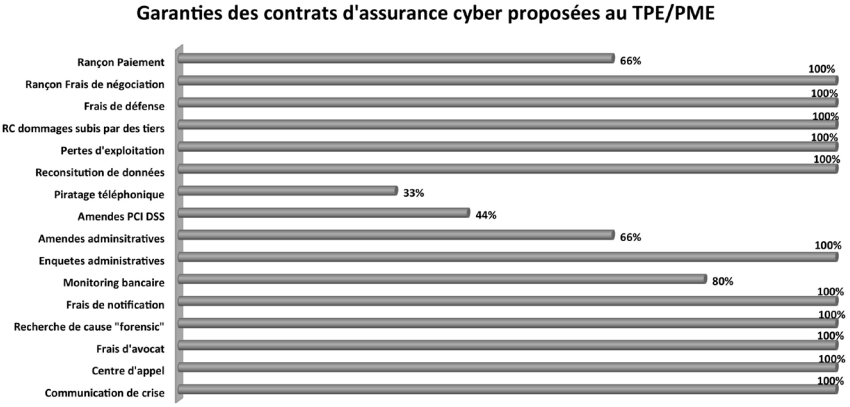
Les contrats cyber sont souvent des contrats multirisques : ils offrent des couvertures de dommages (frais et pertes subis) et de responsabilité civile (dommages immatériels aux tiers), et des services de gestion de crise.

(34) *Loi relative à l'informatique, aux fichiers et aux libertés,* 6 janv. 1978, no 78-17.
(35) *Loi relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale,* 18 déc. 2013, no 2013-1168.

Ces contrats offrent principalement les garanties suivantes.

- Les frais et pertes subis à la suite d'une intrusion malveillante (volet dommage) :
  - Les frais d'expertise informatique (forensic[36] après sinistre)
  - Les frais de gestion de l'incident et de la crise (préservation de l'image)
  - Les frais de reconstitution des données
  - Les frais de réparation du système infecté
  - Les pertes d'exploitation consécutives (sans dommage matériel)
- Les frais à la suite d'une violation de données personnelles :
  - Les frais d'enquête administrative
  - Les frais de notification
- Les conséquences de la responsabilité civile :
  - Les dommages chez des tiers à la suite d'un défaut de sécurité chez l'assuré
  - Les dommages chez des tiers à la suite d'un défaut de protection des données personnelles, bancaires ou de santé de tiers
  - Les frais d'avocat
  - Les frais de défense recours

(36) Recherche de cause.



Les pourcentages font référence à la proportion d'un échantillon d'assureurs représentatifs du marché français de l'assurance cyber proposant ce type de garantie dans leur contrat cyber à destination des TPE/PME (source FFA / 2017).

Focus – Les conséquences sur l'assurance de la loi informatique et libertés no 78-17

du 6 janvier 1978 consolidée et de la loi de programmation militaire no 2013-1168

du 18 décembre 2013 pour la période 2014-2019

La législation en matière de protection des données à caractère personnel ainsi qu'en matière de sécurité des systèmes d'information impose pour certains opérateurs une obligation de notification à une autorité compétente et/ou aux tiers victimes en cas d'incident numérique.

Dans le cadre de la protection des données à caractère personnel, les fournisseurs de services de communications électroniques[37] doivent réaliser cette notification auprès de la Commission nationale de l'informatique et des libertés (CNIL) et des tiers victimes de la violation des données personnelles.

(37) Loi relative à l'informatique, aux fichiers et aux libertés, 6 janvier 1978, no 78-17, art. 34 bis.

Dans le cadre de la réglementation en matière de sécurité des systèmes d'information, les opérateurs d'importance vitale[38] (OIV) doivent réaliser cette notification auprès de l'ANSSI[39] et du Premier ministre en cas d'incident sur leur système d'information.

Ces réglementations prévoient également un pouvoir de contrôle de l'ANSSI sur les systèmes d'information des opérateurs d'importance vitale (OIV)[40] et de la CNIL sur les traitements de données personnelles[41]. En cas d'enquête diligentée par l'une de ces deux autorités de contrôle, les opérateurs doivent mettre leurs ressources à disposition de celles-ci.

Les frais de notification ainsi que les frais d'enquêtes administratives sont pris en charge dans le cadre des contrats dédiés au risque cyber. Lorsque des acteurs sont mis en cause dans le cadre d'une procédure de sanction administrative ou pénale, ils sont amenés à engager des frais de défense qui peuvent aussi être pris en charge dans le cadre des contrats dédiés au risque cyber.

À la suite de ces procédures, l'autorité administrative peut condamner l'entreprise au paiement d'une amende. En France, l'assurance de ces amendes administratives semble contraire à l'ordre public (articles 6 du Code civil, arrêt du 14/02/2012 de la cour d'appel de Paris). Pour autant, tous les assureurs/assurés n'ont pas la même appréciation de la réglementation. Certains assureurs proposent donc, « sous réserve de leur assurabilité » effective, pour les seules personnes physiques et dans le cadre de sous-limites, la couverture des amendes administratives ; d'autres pas.

(38) *Loi relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale*, 18 décembre 2013, no 2013-1168, art. 22.
(39) Agence nationale de sécurité des systèmes d'information (ANSSI).
(40) Idem.
(41) *Loi relative à l'informatique, aux fichiers et aux libertés*, 6 janvier 1978, no 78-17, art. 11.

C. La capacité du marché et les limites actuelles des montants de couverture disponibles

Si l'évolution des contrats traditionnels et le développement des contrats dédiés au risque cyber témoignent d'une meilleure prise en charge du risque cyber par les assureurs, la capacité du marché de l'assurance cyber pur au niveau international, et singulièrement au niveau français, demeure à ce jour limitée.

La capacité globale maximale mobilisable pour un seul contrat est estimée à 500-700 millions d'USD[42].

Si la capacité délivrée par certains assureurs est de l'ordre de 75 à 100 millions d'USD[43], la capacité moyenne par assureur serait d'environ 25 millions d'USD en 2015[44].

Ces niveaux peuvent paraître modestes au regard de l'ampleur du risque auquel les entreprises sont exposées. Ils sont toutefois à mettre en perspective avec, d'une part, les besoins en fonds propres à mobiliser par les assureurs pour faire face à de potentielles cyberattaques de grande ampleur et, d'autre part, la demande encore limitée du marché. Pour le segment des TPE/PME, cette capacité unitaire apparaît suffisante.

Pour le segment des grandes entreprises en revanche, les demandes de capitaux assurables, même avant les changements réglementaires attendus en 2018, sont nettement supérieures à l'offre.

(42) Marsh, *Benchmarking trends : interest in cyber insurance continues to climb,* avril 2014. Le niveau mentionné dans cette étude n'aurait pas évolué depuis.
(43) J. FINKLE., *Cyber insurance premiums rocket after high-profile attacks*, Reuters Technology News, 12 oct. 2015 , [www.reuters.com/article/us-cybersecurity-insurance-insight- idUSKCN0S609M20151012.] ; Insurance Journal, *Munich Re, Beazley Partner to Provide Enhanced Cover for Large Cyber Risks*, 20 Avr. 2017, [http://www.insurancejournal.com/news/international/2017/04/20/448519.htm.] ; FAULKNER M., Mun*ich Re Syndicate targets deeper cyber exposure, Insurance Day,* 13 avr. 2017, [www.insuranceday.com/ece_incoming/munich-re-syndicate-targets-deeper-cyber-exposure.htm.].
(44) Council of Insurance Agents & Brokers, *Cyber Insurance Market Watch Survey: Executive Summary,* oct. 2015.

III. Une demande d'assurance cyber encore bridée

A. Un marché en cours de mutation

Les premiers contrats cyber « purs » sont apparus au début des années 2000 aux États-Unis et ont connu un fort développement grâce à une évolution réglementaire rendant obligatoire la notification de toute violation de ses données personnelles à la personne / l'entité concernée.

Focus – California Data Breach Act (2003) et le marché de la cyber assurance aux États-Unis

Au début des années 2000, l'État de Californie a été victime d'un incident de sécurité ayant causé la divulgation des données relatives aux salaires de plus de 200 000 fonctionnaires.

À la suite de ce vol, la première obligation de notification de faille de sécurité a été introduite en Californie par le « Data breach Notification Act » en 2003[45]. Cette obligation impose aux entreprises ou aux autorités publiques d'informer les personnes concernées en cas de faille de sécurité affectant leurs données à caractère personnel.

Les coûts de notification étant très élevés, les acteurs économiques ont souhaité transférer ce risque financier vers les assureurs, ce qui a fortement accéléré le développement de la cyber-assurance[46]. Plusieurs autres États ont par la suite adopté une législation équivalente.

Un impact comparable est attendu sur le marché européen de la cyber-assurance avec la mise en place du nouveau cadre juridique en matière de protection de données à caractère personnel et de sécurité des systèmes d'information en mai 2018.

(45) K. D. HARRIS , California data breach report, fev. 2016, [https://oag.ca.gov/breachreport2016].
(46) OCDE, *Perspectives de l'économie numérique*, 2015, p. 256.

Aujourd'hui, le marché mondial de l'assurance cyber représente entre 3 et 3,5 milliards d'USD[47].

Le marché américain représente 85 à 90 % des primes annuelles[48]. Le marché européen ne représente que 5 à 9 %[49] du marché mondial, soit un montant maximal d'environ 255 millions d'euros (300 millions d'USD[50]) de primes. Le volume de primes souscrites en France était d'environ 40 millions d'euros en 2016[51].

La pénétration globale de l'assurance cyber est particulièrement complexe à mesurer.

- En Europe, ce marché est en train de se consolider.
- Les rares chiffres disponibles ne capturent généralement que les primes souscrites au titre des contrats cyber dédiés. Les primes des garanties couvrant un fait générateur cyber au sein des contrats traditionnels (de dommages et de responsabilité civile) ne sont alors pas prises en compte.

Selon le dernier baromètre en matière de cybersécurité réalisé par Orange Cyberdéfense en janvier 2017 :

- 73 % des entreprises industrielles françaises interrogées n'étaient pas assurées contre les risques liés aux défaillances de cybersécurité fin 2016 ;
- 32 % d'entre elles envisageaient de s'assurer dans les douze mois contre le cyber-risque ;

(47) Lloyd's, *Counting the Costs, Cyber Exposure Decoded*, Emerging Risk Report 2017, July 2017, p. 8.
(48) Aon Benfield, *Cyber Update : 2016 cyber insurance profits and performance*, 2017 (cette étude souligne en outre que le risque pour les États-Unis est partagé entre des assureurs des États-Unis et des assureurs de Londres et des Bermudes) ; OECD, *Enhancing the Role of Insurance in Cyber Risk Management*, 2017.
http://thoughtleadership.aonbenfield.com/Documents/20170504-ab-cyber-naic-supplemental-study.pdf.
(49) OECD, *Enhancing the Role of Insurance in Cyber Risk Management,* 2017. Ces données, qui ne prennent en compte que les primes de contrats dédiés au risque cyber, résultent d'estimations sur la base d'études ou d'enquêtes réalisées par des entreprises privées. Aucune consolidation officielle n'existe à ce jour.
(50) Marsh, *Continental European Cyber Risk Survey : 2016 Report,* October 2016.
(51) L. THEVENIN, « Le premier vrai test pour un marché de la cyberassurance en plein essor », *Les Échos*, 15 mai 2017, [https://www.lesechos.fr/finance-marches/banque-assurances/0212089405169-le-premier-vrai-test-pour-un-marche-de-la-cyberassurance-en-plein-essor-2086949.php#.].

- 79 % des entreprises de moins de 250 salariés et 60 % des entreprises de plus de 250 salariés[52] n'étaient pas assurées.

Ces chiffres concordent avec ceux de l'étude réalisée en avril 2017[53] par le Cigref[54] auprès de grandes entreprises principalement, qui révèle que seulement 43 % d'entre elles sont couvertes par une assurance cyber.

Les études convergent pour démontrer que les grandes entreprises ont pris conscience du risque cyber et de l'utilité de transférer ce risque vers l'assurance, avec souscription ou non d'une police cyber dédiée. À l'inverse, cette prise de conscience est loin d'être généralisée dans les TPE/PME. Plus l'entreprise est de petite taille, moins elle est informée de la possibilité de transférer ce risque vers un contrat d'assurance.

B. Les principaux freins au développement de la demande

En plus des freins au développement de l'offre d'assurance cyber, mentionnés en partie 1. I, divers obstacles entravent également le développement de la demande.

1. Un déficit de compétences techniques et juridiques qui empêche de nombreux acteurs économiques d'appréhender le risque cyber de façon pertinente

Une majorité d'entreprises, de petite taille en particulier, manque encore de compétences techniques et juridiques à mesure qu'elles se numérisent.

(52) Orange Cyberdéfense, *Baromètre cybersécurité 2017 – Où en est l'industrie française ?*, janv. 2017, p. 15.
(53) Cybersecurity Insights, *Comment « débloquer » le marché de l'assurance cyber en France ?*, juin 2017, p. 10.
(54) Le Cigref est une association créée en 1970 regroupant 140 grandes entreprises et organismes français. Sa mission est de « développer la capacité des grandes entreprises à intégrer et à maîtriser le numérique ».

Selon une récente étude[55] portant sur les États-Unis, l'Angleterre, la France, l'Allemagne, l'Australie, le Japon, le Mexique et Israël, plus de 80 % des entreprises sondées dénoncent un manque de compétences en matière de cybersécurité dans leur organisation, et 75 % en France ; un tiers pensent que ce déficit fait de leur organisation des cibles privilégiées de piratage ; un peu moins d'un quart lui attribuent des dommages en termes de réputation et la perte de données du fait d'attaques cyber.

Une autre étude[56] analysant des données d'organisations basées en Amérique du Nord et dans les régions EMEA et Asie Pacifique conclut que 46 % des organisations interrogées en 2017 estiment avoir un « déficit problématique » de compétences en matière de cybersécurité. La progression de ce taux sur deux ans est la donnée la plus révélatrice : elles n'étaient que 28 % à établir le même diagnostic en 2015, ce qui prouve probablement que les organisations sont plus conscientes du risque mais n'ont pas pour autant ajusté leurs compétences.

Le déficit de compétences techniques sur le risque cyber se double souvent d'un déficit de veille et de compétences juridiques. Il entrave la compréhension des nouvelles obligations qui incombent aux organisations et la mise en conformité. La préparation de la mise en œuvre du règlement européen en matière de protection des données et celle de la directive NIS sont, à cet égard, des baromètres révélateurs. 97 % des entreprises européennes auraient entendu parler du règlement européen relatif à la protection des données à caractère personnel, mais 57 % d'entre elles ne connaissent pas ou très peu ses implications[57].

Ce déficit de compétences est un obstacle au déploiement de solutions de cybersécurité adaptées à l'exposition au risque. Il explique aussi que beaucoup d'entreprises n'envisagent pas de mettre en place une couverture financière du risque cyber, par le transfert de ce risque à l'assurance, le cas échéant.

(55) Intel Security, en partenariat avec le Center for Strategic and International Studies (CSIS), *Hacking the Skills Shortage,* 2016.
(56) ESG, ISSA, Through the Eyes of Cyber Security Professionals : An Annual Research Report (Part II), 2017.
(57) Lloyd's, *Faire face aux menaces cyber,* 20 sept. 2016, p. 5.

Sur le segment des ETI et des grandes entreprises, l'AMRAE fournit un important travail pour sensibiliser ses adhérents à ce sujet. L'AMRAE a développé des outils d'analyse de risques qui seront présentés dans le cahier dédié au risk management et à la prévention/protection.

2. Une sous-estimation du risque cyber

Une large majorité d'entreprises continue à sous-estimer le risque cyber. Si la plupart d'entre elles sont conscientes de l'existence du risque, elles ne s'estiment pas nécessairement exposées, comme le reflètent différentes études. Selon une étude de PwC de 2016[58], « le risque de cybercriminalité est aujourd'hui encore peu appréhendé par les entreprises françaises, toutes tailles confondues (sachant que plus de 99 % des entreprises françaises sont des microentreprises et des PME[59]) : seules 17 % s'y sentent exposées, principalement au sein des entreprises du secteur industriel ». En décembre 2016, le cabinet Denjean et associés relevait que seulement 38 % des entreprises françaises estimaient que leur risque de subir une cyberattaque était important ou très important[60].

Sur le segment des TPE/PME, en particulier, une majorité d'entreprises estime qu'elles ont peu de chance d'être victimes d'incidents cyber, notamment lorsqu'elles externalisent la maintenance de leur système d'information et l'hébergement de leurs données auprès de prestataires sans avoir conscience des risques problématiques associés à ce choix. Pourtant, d'après l'Internet Security Report 2016 de Symantec, elles représenteraient 77 % des victimes d'attaques numériques en France.

(58) PwC, *Le marché de la cyber-assurance : la révolution commence maintenant*, janv. 2016 p. 7.
(59) Insee, données pour l'année 2015 parues le 6 octobre 2017 ; https://www.insee.fr/fr/statistiques/2016091.
(60) Denjean et associés, *Les entreprises françaises face aux cyber-attaques,* déc. 2016. p. 4.

3. Une méconnaissance des couvertures d'assurance des risques cyber

Parce qu'ils sous-estiment leur exposition à ce risque difficile à appréhender, la plupart des acteurs économiques n'envisagent pas la possibilité de son transfert à l'assurance.

De surcroît, beaucoup ignorent encore l'existence de contrats d'assurance spécifiques pour se prémunir contre la survenance d'un incident cyber. Ainsi, selon une étude du Lloyd's[61], 73 % des dirigeants d'entreprises européennes n'auraient qu'une connaissance limitée de l'assurance cyber, et 50 % d'entre eux n'auraient pas connaissance de l'existence de garanties risques cyber en cas de fuites de données.

Nombre d'entreprises méconnaissent également le périmètre des couvertures cyber, atomisées entre plusieurs types de contrats (voir II), ce qui constitue un frein important à la souscription d'assurance à plusieurs titres.

- La complexité de la couverture cyber liée à la multiplication des polices, la possibilité de leur chevauchement, les restrictions et exclusions, en plus de la technicité du risque lui-même et de ses conséquences pour l'entreprise, peuvent décourager certaines entreprises de souscrire une assurance alors qu'elles ne sont pas certaines de leur étendue en termes de garantie, de limite et de franchise.
- La difficulté de comparaison des offres de différents prestataires constitue un obstacle supplémentaire à la souscription. Dans un contexte d'évolution rapide du risque et des offres d'assurance, les termes et les conditions des polices d'assurance cyber varient substantiellement. Même la définition d'éléments clés des couvertures peut varier : celle du « système informatique » peut inclure ou non les systèmes d'un gestionnaire de données en nuage externalisé, par exemple.
- Aussi, en l'absence de clarification sur le périmètre de couverture de leurs contrats en matière de cyber-risques, beaucoup d'entreprises se croient, à tort, protégées contre la totalité des conséquences

(61) Lloyd's, *Faire face aux menaces cyber,* 20 sept. 2016, p. 5.

dommageables du cyber-risque et ne voient pas l'utilité de la souscription d'un contrat dédié ou d'une extension de contrats traditionnels. Pourtant, la décision rendue par la Cour suprême de New York dans le cadre, notamment, de la demande d'indemnisation de Sony est une incitation à la prudence et à la pratique d'audits détaillés des couvertures cyber pour éviter de ne prendre la mesure des lacunes dans la couverture qu'après une attaque de grande ampleur.

Focus – Les enseignements de la jurisprudence Sony

En 2011, Sony PlayStation Network a fait l'objet d'un piratage de grande ampleur : 80 millions de données d'utilisateurs ont été dérobées.

À la suite de cette attaque, Sony a réclamé à ses assureurs, sur le fondement de son contrat de responsabilité civile, le remboursement des sommes déboursées dans le cadre des obligations de notification en vigueur. Une procédure a été lancée par Sony à la suite du refus de prise en charge du sinistre par les assureurs.

La Cour suprême de New York a finalement rejeté la demande d'indemnisation réclamée par Sony Corporation à ses compagnies d'assurances au titre de la responsabilité civile : elle a considéré que la police d'assurance responsabilité ne couvrait pas les préjudices personnels ou imputables à la publicité résultant du vol de données à caractère personnel par des pirates informatiques. L'entreprise victime des pirates ne disposait alors d'aucune couverture en cas de cyberattaque.

La Cour a considéré que les frais de notification n'étaient pas couverts par les contrats traditionnels, ni en dommage, ni en responsabilité civile.

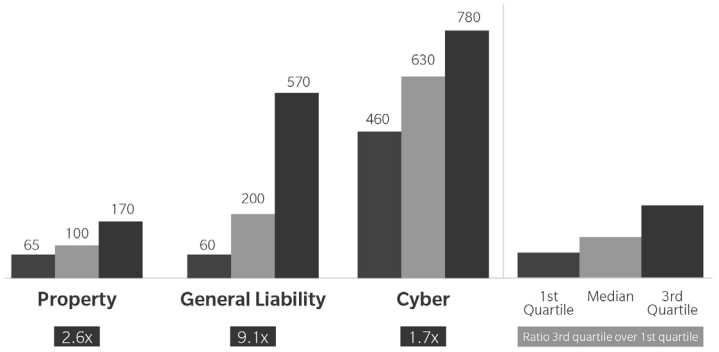
Une exclusion standard des contrats RC a depuis été mise en place aux États-Unis pour clarifier l'étendue des couvertures et éviter à d'autres entreprises de connaître l'expérience de Sony.

4. Des primes insuffisamment corrélées au risque

Comme sur tous les marchés immatures, la quantification du risque est soumise à de nombreuses incertitudes : absence de statistiques sinistre, méconnaissance technique de la vulnérabilité des risques, absence de certitudes en matière de prévention et de protection…

Les difficultés de quantification du risque se reflètent dans une segmentation tarifaire limitée. Un rapport de Marsh, en 2015[62], mettait en évidence que la branche cyber connaissait des écarts de primes faibles en comparaison des branches de dommages et de responsabilité civile.

Focus – Analyse des primes pour les contrats cyber, dommages aux biens et responsabilité civile



Source : UK Cyber security : The Role of Insurance in Managing and Mitigating the Risk – Marsh 2015

Les mesures mises en place par les assurés et prospects pour renforcer leur sécurité numérique peuvent être insuffisamment prises en compte dans les niveaux de primes[63].

(62) Marsh, *UK cybersecurity, the role of insurance in managing and mitigating the risk,* Marsh 2015, p. 22.
(63) O. BOGOMOLNIY, *Cyber Insurance Conundrum: Using CIS Critical Security Controls for Underwriting Cyber Risk,* publishes by The SANS Institute, 2017, p. 8.

Les ajustements tarifaires peuvent se faire par le biais de franchises, de limites et de chargements de sécurité.

Dès lors, le niveau de prime au regard de l'appréciation de la couverture est souvent cité comme l'un des obstacles importants à la souscription d'assurance cyber[64].

(64) Voir par exemple PwC, *Insurance 2020 & beyond, Reaping the dividends of cyber resilience,* 2015, p. 11 : « Many insurers are also setting limits below the levels sought by their clients (the maximum is $500 million, though most large companies have difficulty securing more than $300. Insurers may also impose restrictive exclusions and conditions. Some common conditions, such as state-of-the-art data encryption or 100% updated security patch clauses, are difficult for any business to maintain. Given the high cost of coverage, the limits imposed, the tight attaching terms and conditions and the restrictions on whether policyholders can claim, many policyholders are questioning whether their cyber insurance policies are delivering real value. »

PARTIE 2
Optimiser l'offre assurancielle pour répondre aux évolutions récentes de l'environnement juridique et de marché

Depuis plusieurs mois, une conjonction de facteurs a contribué à créer un environnement favorable au développement de la couverture du risque cyber. Il appartient maintenant aux différents acteurs concernés de prendre en compte cette dynamique pour développer des produits d'assurance moins complexes et plus flexibles, répondre à une demande appelée à une croissance rapide, et contribuer à renforcer la résilience de l'économie nationale face à un risque cyber croissant.

I. Un nouvel environnement économique et réglementaire favorable à la couverture du risque cyber...

On peut identifier quatre leviers principaux qui portent aujourd'hui la demande de protection financière contre le risque cyber : une prise de conscience du risque qui s'est accélérée ces derniers mois, une évolution du régime de responsabilité civile en France, une uniformisation du cadre juridique européen, et une incitation à une prise en compte croissante du risque cyber dans la gouvernance des entreprises. D'autre part, les travaux d'harmonisation des définitions et des catégorisations des

risques cyber, et, en France, la clarification de l'étendue de la couverture du Gareat dans le cas du cyberterrorisme, lèvent également des freins au développement de l'assurance cyber.

A. Une prise de conscience croissante du risque

Malgré des taux de souscription encore peu élevés, notamment pour les TPE/PME et les collectivités locales, les derniers indicateurs traduisent un progrès dans la prise de conscience du risque cyber. En témoigne notamment le fait que, dans 64 % des entreprises de moins de 250 salariés, les investissements de cybersécurité devraient être en hausse sur les douze prochains mois[65].

La récente cascade d'incidents cyber majeurs a certainement fortement contribué à accélérer cette prise de conscience du risque. Quatre caractéristiques des récentes attaques ont fait réaliser à de nombreux acteurs que les prestataires informatiques ou acteurs de l'économie 2.0 (fournisseurs d'accès à Internet, start-up informatique, SSI…) n'étaient pas les seules victimes potentielles, et que la mise en place d'une protection technique et financière était utile, voire vitale, pour de nombreuses entreprises (une large part des TPE/PME ne survivent pas à une attaque cyber).

- La diversité des acteurs touchés – À titre d'exemple, l'attaque WannaCry a touché des institutions d'origines très variées, et ce, dans le monde entier : des hôpitaux anglais appartenant au service public de santé, le livreur américain FedEx, le ministère russe de l'Intérieur, l'opérateur télécom espagnol Telefónica, la compagnie ferroviaire Deutsche Bahn, etc.
- Le coût des attaques pour les acteurs touchés – Maersk, par exemple, a annoncé mi-août un coût prévisionnel qui pourrait atteindre 300 millions d'euros[66], avec une très large part due à l'interruption d'activité.

(65) Orange Cyberdéfense, *Baromètre cybersécurité 2017 – Où en est l'industrie française ?*, janv. 2017, p. 17.
(66) Zdnet, *Ransomware Petya : un colis à 300 millions de dollars pour Maersk,* 17 août 2017, [www.zdnet.fr/actualites/ransomware-petya-un-colis-a-300-millions-de-dollars-pour-maersk-39856172.htm].

- La réaction coordonnée de certaines victimes – Estimant qu'Equifax n'avait pas suffisamment protégé leurs informations, de nombreux clients (particuliers, entreprises et États fédérés) ont déposé plainte contre la société. Des actions collectives sont envisagées, qui seraient parmi les plus importantes du genre dans l'histoire américaine pour ce qui est du nombre de personnes concernées[67].
- L'importante médiatisation de ces événements.

Cette récente prise de conscience doit aussi beaucoup au travail d'éducation des entreprises, collectivités et associations, porté par les acteurs compétents en matière de risque cyber : l'ANSSI, l'AMRAE, les fédérations professionnelles, ainsi que les prestataires de services informatiques et conseils spécialisés en risque cyber. Parmi ces initiatives, on mentionnera notamment :

- le Guide d'hygiène informatique, publié en 2017, par l'ANSSI[68], proposant 42 mesures et ayant pour objectif d'accompagner les responsables de la sécurité des systèmes d'information ;
- la plate-forme « cybermalveillance.gouv.fr » de l'ACYMA (lancée le 30 mars 2017 par le groupement d'intérêt public du même nom), qui permet d'apporter une assistance aux victimes de cyber-malveillance, et de sensibiliser le public aux enjeux de la sécurité et de la protection de la vie privée ;
- le MOOC « SECNUMACADEMIE », plate-forme de formation à la sécurité numérique de l'ANSSI, ouverte à tous et gratuite ;
- le guide de sensibilisation de la FFA à destination des TPE/PME, « Anticiper et minimiser l'impact d'un cyber-risque sur votre entreprise : TPE, PME, vous êtes concernées ! », publié en mai 2017 ;

(67) *L'Express, L'Expansion,* « Equifax : enquête du régulateur américain du commerce après le piratage », 14 sept. 2017, [http://lexpansion.lexpress.fr/actualites/1/actualite-economique/equifax-enquete-du-regulateur-americain-du-commerce-apres-le-piratage_1943639.html].
(68) ANSSI, *Guide d'hygiène informatique,* [https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/].

- les travaux dédiés et les contributions de l'AMRAE :
  - > Cyber-risques : outil d'aide à l'analyse et au traitement assurantiel[69],
  - > la gestion du risque numérique dans l'entreprise[70],
  - > le livre blanc « La maîtrise du risque cyber sur l'ensemble de la chaîne de sa valeur et son transfert vers l'assurance »[71],
  - > le document conjoint[72] entre FERMA[73] et ECIIA[74] sur la cyber-gouvernance.

Cette sensibilisation au risque cyber vise tous les niveaux de l'entreprise, y compris les directions générales, qui doivent veiller à ce que les mesures de prévention imposées à l'ensemble des salariés soient respectées par tous, quel que soit le niveau hiérarchique, y compris par elles-mêmes.

B. L'élargissement du champ des obligations et de la responsabilité des entreprises

L'entrée en vigueur, en mai 2018, d'un nouveau régime juridique de responsabilité en matière de protection des données à caractère personnel et de sécurité des systèmes d'information, au niveau européen, alourdit potentiellement considérablement le coût d'attaques cyber pour les entreprises. La demande de souscription de polices d'assurance cyber, qui couvrent tant les frais de notification des incidents (dont l'obligation a été étendue) que la mise en cause de la responsabilité de l'entreprise par les victimes (qui pourrait devenir plus fréquente), devrait s'en trouver stimulée.

(69) AMRAE, *Cyber-risques : outil d'aide à l'analyse et au traitement assurantiel*, cahier technique, mars 2015 [http://www.amrae.fr/cyber-risques-outil-daide-%C3%A0-lanalyse-et-au-traitement-assurantiel].
(70) AMRAE, *La gestion du risque numérique en entreprise*, février 2014 [http://www.amrae.fr/la-gestion-du-risque-num%C3%A9rique-dans-lentreprise], collection « Dialoguer AMRAE » mise à jour janvier 2018.
(71) GT System X, [http://www.irt-systemx.fr/v2/wp-content/uploads/2016/11/ISX-IC-EIC-transfert-risque-LIV-0401-v10_2016-10-25.pdf].
(72) Cyber Risk Governance report[http://www.ferma.eu/exclusive-ferma-eciia-cyber-risk-governance-report-available?type=advocacy].
(73) Federation of European Risk Management Associations (FERMA).
(74) European Confederation of Institutes of Internal Auditing (ECIIA).

1. L'obligation de notification

La généralisation de l'obligation de notification en matière de violation de données à caractère personnel et l'extension du champ d'application de l'obligation de notification des incidents de sécurité des systèmes d'information devraient avoir un double impact sur l'activité d'assurance.

a. L'accroissement attendu des frais de notification et de la mise en cause de la RC des entreprises

À l'heure actuelle, l'obligation de notification pour les victimes d'incident cyber, en cas d'atteinte à la sécurité des données ou des systèmes d'information, est limitée aux opérateurs d'importance vitale (OIV) en cas d'incidents affectant le fonctionnement ou la sécurité des systèmes d'information[75], et aux fournisseurs de services de communication électronique en cas de violation des données à caractère personnel[76].

À compter du 25 mai 2018, cette obligation de notification sera étendue à toutes les entreprises ayant des activités de traitement des données[77].

Quant à l'obligation de notification des incidents de sécurité des systèmes d'information, elle concernera, outre les opérateurs d'importance vitale, les opérateurs de services essentiels et les fournisseurs de service numérique[78].

(75) *Loi no 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale,* art. 22.
(76) *Loi relative à l'informatique, aux fichiers et aux libertés,* 6 janv. 1978, no 78-17, art. 34 bis.
(77) *Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données),* 27 avril 2016, 2016/679.
(78) *Directive (UE) du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union,* 6 juil. 2016, 2016/1148, art. 14, art. 16.

Notification d'incidents dans le cadre de la directive NIS[79]

Directive sur la sécurité des réseaux et des systèmes d'information, connue sous l'appellation « Directive NIS – Network and Information Security »

Comme pour la loi de programmation militaire ou le règlement général pour la protection des données, la directive NIS (article 14) prévoit l'obligation de notification des incidents ayant un impact sur la continuité de leurs services essentiels auprès de l'autorité nationale pour tous les opérateurs de services essentiels (OSE).

Pour les fournisseurs de services numériques (FSN), l'article 16 de la directive précise expressément que l'obligation de notification ne doit être appliquée que lorsque le fournisseur de service numérique a accès aux informations nécessaires pour évaluer l'impact de l'incident eu égard, en particulier, aux paramètres suivants :

- le nombre d'utilisateurs touchés par l'incident, en particulier ceux qui recourent au service pour la fourniture de leurs propres services ;
- la durée de l'incident ;
- la portée géographique, eu égard à la zone touchée par l'incident ;
- la gravité de la perturbation du fonctionnement du service ;
- l'ampleur de l'impact sur les fonctions économiques et sociétales.

Pour les OSE, comme pour les FSN, la notification au public est limitée aux cas où il serait dans l'intérêt général de divulguer l'incident.

Comme pour les obligations en matière de sécurité, ces dispositions ne sont pas applicables aux microentreprises et aux petites entreprises.

(79) *Directive (UE) du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union*, 6 juil. 2016, 2016/1148, art. 14, art. 16.

Les frais de notification engagés pour informer les tiers de la violation des données personnelles comprennent de nombreux postes de charges, notamment les coûts relatifs aux activités informatiques de mises à jour de bases de données, à la mise en conformité avec les exigences réglementaires, au recrutement d'experts externes, aux frais postaux, à la configuration des contacts secondaires à prévenir par courrier, au retour d'e-mails et aux communications entrantes. Le montant, potentiellement très élevé, de ces coûts constitue une forte incitation à souscrire une assurance cyber pour en transférer le risque à l'assureur.

De plus, avant la généralisation de l'obligation de notification des violations des données, les victimes n'avaient pas connaissance des divulgations de leurs données et ne pouvaient mettre en cause la responsabilité d'une entreprise victime d'une attaque.

À compter de mai 2018, date à laquelle les notifications mentionneront expressément la nature des données compromises, les tiers victimes ayant connaissance de cette violation seront amenés à mettre en cause plus facilement la responsabilité de l'entreprise cible de l'attaque pour demander la réparation de leurs préjudices. Les contrats d'assurance RC seraient donc davantage sollicités.

b. L'enrichissement des bases de données sur les incidents cyber et leur gestion

Avec l'obligation de notification et le possible transfert de ses frais de mise en œuvre vers l'assureur, le nombre de réclamations enregistrées et de sinistres payés devrait augmenter. Les bases de données des assureurs devraient donc gagner en profondeur. Une collaboration sur ce sujet entre la CNIL, qui enregistre les notifications, et l'assureur, qui prend en charge les indemnisations associées, permettrait, sous condition d'une définition et d'un calibrage pertinent des incidents à reporter, d'améliorer substantiellement l'appréhension du risque cyber.

L'enrichissement des portefeuilles assurés permettra également une meilleure segmentation par taille et secteur d'activité des entreprises assurées, une meilleure connaissance de la sinistralité et de meilleures corrélations

avec les mesures de prévention et de protection, ainsi qu'une approche tarifaire plus adaptée à la réalité du risque (voir ci-dessous). L'ensemble de ces facteurs concourra à une gestion optimisée de ce risque par les assureurs et les réassureurs, qui pourront ainsi proposer aux entreprises une offre de produits plus sophistiquée.

2. Un risque accru d'engagement de la responsabilité des entreprises

Le règlement européen en matière de protection des données à caractère personnel, qui sera applicable à compter du 25 mai 2018, marque un changement dans l'encadrement du traitement des données à caractère personnel.

Ce texte est fondé sur la responsabilisation, ou « accountability », des acteurs dans leur activité de traitement des données à caractère personnel, ce qui se traduit en France par la suppression des formalités préalables aux traitements de données remplacées par un renforcement des mécanismes de contrôles et de mise en cause de la responsabilité des responsables de traitement.

a. Responsabilité civile

En renforçant les obligations à la charge du responsable de traitement, le règlement européen en matière de protection des données personnelles va augmenter les risques de mise en cause de la responsabilité civile de l'entreprise du fait d'un cyber-événement. Dans le cadre de ses relations contractuelles, son exposition au risque sera d'autant plus élevée que le fait générateur cyber est susceptible de causer des dommages en cascade à de nombreux acteurs de l'ensemble de la chaîne de valeur (ex. : arrêt d'une chaîne de production, absence de production, absence de livraison d'un produit, interruption brutale de relations commerciales…).

Ce renforcement des mécanismes de responsabilité des responsables de traitement impacte directement les contrats d'assurance de responsabilité civile. Ceux-ci interviennent pour indemniser les conséquences

pécuniaires consécutives à la mise en cause de la responsabilité des victimes d'un incident numérique par les tiers sous réserve d'exclusions spécifiques prévues au contrat.

b. Responsabilité des dirigeants

L'entrée en vigueur au 25 mai 2018 du régime de responsabilité issu du règlement européen sur la protection des données personnelles (RGPD) et les fortes sanctions infligées par les autorités régulatrices (notamment la CNIL) – pouvant atteindre 20 millions d'euros ou 4 % du chiffre d'affaires mondial, la valeur la plus élevée étant retenue – en cas de non-notification par les responsables de traitement des violations de données personnelles inciteront probablement les entreprises à investir :

- dans la prévention, en mettant en place des mesures de sécurité au sein de leurs systèmes d'information ;
- dans la protection, grâce à la souscription de couvertures d'assurances cyber-risques.

S'en abstenir pourrait, le cas échéant, être constitutif d'une faute de gestion entraînant la responsabilité du dirigeant de l'entreprise victime d'un incident cyber, notamment si ce manquement devait impacter significativement les résultats, voire la pérennité de la société.

Focus – État des poursuites contre les dirigeants de la chaîne de supermarché « Target »

Le vol, en 2013, de 110 millions de données personnelles (dont des données bancaires) des clients de la chaîne de supermarché « Target » a généré plus de 80 poursuites judiciaires et actions collectives (class actions), y compris à l'encontre de ses dirigeants.

La dernière évaluation du coût de ces réclamations, communiquée par l'assureur chargé de couvrir la responsabilité personnelle des dirigeants, s'élève, en octobre 2017, à 65 millions d'USD de frais de défense et d'investigation.

Par ailleurs, l'entrée en vigueur de la loi no 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre impose un contrôle plus important de ces dernières sur leurs sous-traitants, notamment en matière de cyber-risque.

En effet, se trouve désormais instaurée par les articles L. 225-102-4 et 5 du Code de commerce une obligation de mise en place effective d'un plan de vigilance comportant des mesures propres *« à identifier les risques et à prévenir les atteintes graves envers les droits humains et les libertés fondamentales, la santé et la sécurité des personnes, ainsi que l'environnement, résultant des activités de la société et de celles qu'elle contrôle (…), ainsi que des activités des sous-traitants ou fournisseurs avec lesquels est entretenue une relation commerciale établie »*.

Même si cette obligation ne pèse pour l'heure que sur les entreprises employant plus de 5 000 salariés avec un siège social en France, ou employant plus de 10 000 salariés avec un siège social en France ou à l'étranger, il n'en demeure pas moins que ce devoir de vigilance étendu (incluant notamment la protection des données personnelles, la protection des systèmes par rapport aux risques cyber, etc.) sera délicat à assumer sur un périmètre aussi vaste, étant précisé que :

- la notion de contrôle est définie par l'article L. 233-16 du Code de commerce, qui englobe non seulement la détention de la majorité des droits de vote et la désignation de la majorité des membres des organes dirigeants, mais aussi le droit d'exercer une influence dominante sur une entreprise en vertu d'un contrat ou de clause statutaire ;
- le concept de sous-traitance est visé par l'article 1er de la loi no 75-1334 du 31 décembre 1975, qui la caractérise par « l'opération par laquelle un entrepreneur confie par un sous-traité, et sous sa responsabilité, à une autre personne appelée sous-traitant l'exécution de tout ou partie du contrat ou du marché public conclu avec le maître d'ouvrage » ;
- Pour déterminer si une relation commerciale peut ou non être qualifiée d'établie, la jurisprudence prend en compte plusieurs critères tels que la durée des relations entre les partenaires, la continuité de celles-ci ou encore l'importance et l'évolution du chiffre d'affaires réalisé. Une succession de contrats ponctuels peut suffire à carac-

tériser une relation commerciale établie à condition d'être significative, régulière et stable.

À défaut d'identifier, de prévenir et de mettre en place toutes mesures utiles destinées à éviter ou à limiter l'impact d'un tel sinistre (par la souscription d'assurances dédiées notamment), les dirigeants d'entreprises pourraient voir leur responsabilité engagée pour défaut d'exercice de leurs obligations de contrôle, de vigilance et de respect des lois et règlements. Cette menace devrait se traduire par un intérêt accru pour les assurances cyber et de responsabilité des dirigeants des entreprises visées par ce nouveau régime.

3. L'uniformisation attendue du cadre juridique au niveau européen

La dématérialisation des échanges et des activités entre États a suscité de nombreuses interrogations quant au droit applicable en matière de protection des données personnelles et de sécurité des systèmes d'information.

Le nouvel environnement juridique mis en place à partir de mai 2018 par la directive « NIS » et le règlement européen RGPD, unifie le cadre juridique applicable.

- L'article 1 de la directive NIS précise que son champ d'application s'étend à l'ensemble des États membres de l'Union.
- L'article 3 alinéa 1 du règlement prévoit son application à l'ensemble des « traitements des données à caractère personnel effectués dans le cadre des activités d'un établissement, d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union ».
- L'alinéa 2 du même article étend le champ d'application de la réglementation en matière de protection des données personnelles aux responsables du traitement ou aux sous-traitants qui ne sont pas établis dans l'Union[80]. Cette extension protège les particuliers

(80) Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/CE (règlement général sur la protection des données), art. 3.

contre les pratiques des opérateurs exploitant les données à caractère personnel depuis l'étranger.

Cette unification est un élément favorisant la mise en place d'une assurance cyber pouvant intervenir au-delà des frontières pour des sinistres « déterritorialisés ». De plus, elle simplifie la pratique des assureurs, qui n'auront besoin de maîtriser qu'un seul cadre juridique.

Focus – L'incidence du RGPD sur les actions de groupe en matière de protection des données

L'action de groupe a fait son entrée en droit français en 2014[81]. Reprise sous le nom de « représentation des personnes concernées » par l'article 80 du règlement européen relatif à la protection des données, cette nouvelle pratique présente un véritable enjeu pour le développement de l'assurance du risque cyber. Cet article permet notamment l'exercice du droit de représentation pour obtenir réparation, comme prévu à l'article 82 dudit règlement.

Toutefois, l'article 80 du règlement prévoit que le droit d'obtenir réparation par représentation ne peut être exercé que lorsque le droit d'un État membre le prévoit.

En 2016, la loi pour la modernisation de la justice, a introduit à l'article 43 ter de la loi informatique et libertés de 1978 l'action de groupe en matière de protection des données. Une telle action ne peut être utilisée qu'afin de faire cesser les manquements aux règles en matière de protection des données, et non pas pour obtenir réparation.

En l'état actuel de la législation, l'action de groupe en matière de protection des données à caractère personnel ne permet donc pas de demander réparation des préjudices subis. Une entreprise pourra toutefois faire face à des actions individuelles en réparation facilitées par une condamnation préalable au titre d'une action de groupe.

(81) Cf. chapitre 1.

C. La prise en compte du risque cyber, critère de bonne gouvernance de l'entreprise

La gestion du risque cyber est de plus en plus considérée comme un indicateur de bonne gouvernance d'entreprise, et non plus uniquement comme un sujet technique relevant de la seule direction informatique.

FERMA[82] et ECIIA[83] ont uni leurs efforts pour produire conjointement un rapport qui présente des recommandations sur la mise en place de cette bonne gouvernance dans les organisations. Ce rapport milite en faveur de la création d'un groupe de gouvernance du cyber-risque, qui, sous la présidence du risk manager, rassemblerait les représentants clés du business et de la sécurité, des premières et deuxièmes lignes de défense, tel que décrit dans le standard ERM[84].

Ce groupe pourra avoir pour mission de quantifier l'exposition financière de l'entreprise au risque cyber et d'y associer des propositions de remédiation adaptées. Cette approche permettra à l'équipe dirigeante de pouvoir comprendre clairement l'exposition de l'entreprise au risque cyber dans l'ensemble de ses dimensions techniques, juridiques et métier, et de pouvoir également allouer les ressources de l'entreprise dédiée à la prévention dans le cadre d'un plan de gestion de risque global[85].

(82) Federation of European Risk Management Associations (FERMA).
(83) European Confederation of Institutes of Internal Auditing (ECIIA).
(84) Entreprise Risk Management (ERM).
(85) Cf. Cahier Prévention, à paraître.

Focus – L'évaluation du cyber-risque dans l'analyse crédit : le point de vue de Moody's

Le cyber-risque, ou l'importance croissante de ce paramètre dans l'analyse crédit

Le cyber-risque recouvre un large éventail de menaces, depuis les attaques par déni de service sur Internet au vol de données, en passant par la perturbation des services d'infrastructure essentiels. Évaluer la capacité de réaction d'une entité émettant de la dette (« émetteur ») face au cyber-risque est difficile au sens où celui-ci est complexe et évolue très rapidement. Il existe, en outre, très peu d'informations publiques, tant sur les mesures de cybersécurité que sur les cyber-événements. Par ailleurs, lorsque celles-ci sont disponibles, un émetteur n'est généralement pas comparable aux autres. Nous prenons en compte le risque d'un cyber-événement de grande ampleur de la même manière que nous abordons le risque de tempêtes ou de catastrophes naturelles, dans la mesure où l'on ne peut déterminer précisément le moment auquel il est susceptible de se matérialiser et où une attaque réussie a des conséquences difficiles à déterminer. Nous avons examiné dans un précédent rapport (*« Cyber risk of growing importance to credit analysis »*, novembre 2015) comment notre analyse-crédit intègre l'évolution rapide du cyber-risque dans un certain nombre de secteurs d'activité.

La gravité et la durée d'une cyber-menace déterminent la manière dont nous intégrons ce risque dans nos analyses et notations. En d'autres termes, le risque de cyberattaque n'est pas explicitement pris en compte dans notre analyse de crédit comme un facteur principal de notation. Néanmoins, dans tous les secteurs d'activité, notre analyse intègre de nombreux scénarios de stress-tests (tests de résistance), et un cyber-événement, au même titre que les autres événements exceptionnels, pourrait constituer le déclencheur de ces scénarios. La gravité et la durée d'un cyber-événement « réussi » seront essentielles pour déterminer son incidence éventuelle sur la qualité de crédit des émetteurs.

Des cyber-risques variables d'un secteur d'activité à l'autre. Les principales menaces auxquelles sont confrontés les secteurs où sont concentrés des volumes importants de données personnelles sont les attaques impliquant le vol de données à grande échelle, susceptibles de se traduire par une atteinte sérieuse en termes de réputation et d'impact financier. Parmi les secteurs exposés à ces risques, on peut citer les intermédiaires et les établissements financiers, les établissements de santé et d'enseignement supérieur, les réseaux sociaux et le secteur de la distribution. Les secteurs d'infrastructure considérés comme essentiels sont exposés à un cyber-risque de nature différente, qui se traduira par une interruption prolongée des services concernés. Cela est susceptible d'avoir plus largement des répercussions économiques et sociales propres à mettre en difficulté les États ou les collectivités locales. Parmi les secteurs les plus exposés à ces risques figurent notamment l'industrie des télécoms et de la chimie, le secteur des transports, les services bancaires, mais aussi les services d'utilité publique.

Intensification du cyber-risque parallèlement au développement de la connectivité Internet. La connectivité Internet, qui constitue un point d'entrée pour les pirates informatiques, s'étend rapidement à de nouveaux produits, appareils et services, tels que l'automobile, les pompes à eau et les installations de chauffage domestique. La progression de cette nouvelle phase du développement d'Internet, appelée l'« Internet des objets », vers plus de produits et plus d'appareils ouvre de nouveaux marchés. En conséquence, le cyber-risque est appelé à devenir de plus en plus présent, et nous allons être amenés à accorder une place de plus en plus prioritaire à ce paramètre dans nos évaluations et analyses de crédit.

Entreprises et institutions renforcent leur gouvernance et augmentent leurs dépenses en matière de sécurité informatique, même si accroître les dépenses n'est pas un gage de fiabilité absolue. Dans tous les secteurs d'activité, le cyber-risque revêt une priorité croissante en termes de gouvernance. Les membres des conseils d'administration renforcent leur expertise en matière de cybersécurité, et nous nous attendons à ce que les émetteurs soient nombreux à mettre en place des sous-comités dédiés à la sécurité informatique, élément que nous jugeons positif pour la qualité de crédit.

Les services d'infrastructure dits essentiels bénéficieront d'une intervention exceptionnelle des gouvernements. Une cyberattaque à grande échelle réussie portant sur des actifs ou des services d'infrastructure essentiels entraînerait, selon nous, une réaction des gouvernements. Celle-ci pourrait prendre la forme d'une intervention exceptionnelle visant à stabiliser une économie régionale, ou à rétablir des libertés individuelles. Aux États-Unis, le Département américain de la sécurité intérieure définit les secteurs d'infrastructure essentiels comme étant les suivants : eau et assainissement, énergie, services d'urgence, services financiers, soins de santé, systèmes de communication, technologies de l'information, transports, nucléaire, chimie et édifices gouvernementaux.

Dans ce cadre, la souscription d'une assurance cyber, qui témoigne de la prise en compte de ce risque par l'entreprise, est considérée comme un élément de bonne gouvernance.

D. Vers une harmonisation des définitions et catégorisations des risques cyber ?

Afin de dissiper les éventuelles incompréhensions liées à la multiplicité des couvertures pouvant intervenir dans le transfert du risque cyber vers l'assurance, il est impératif de clarifier, au niveau du marché, les définitions des cyber-risques.

En Europe, un tel travail a été lancé par :

- le Cambridge Center for Risk Studies[86] dans le cadre d'un partenariat privé-public de production, auquel l'université de Cambridge a pris part, avec la production de définitions médianes et communes à l'ensemble des parties participant au partenariat ;
- le CRO forum[87], réunissant les « Chief Risk Officers » des grandes sociétés d'assurance et de réassurance européennes ; celui-ci a publié également, en juin 2016, un rapport proposant une méthodologie de catégorisation des risques cyber[88] ; cette méthodologie offre une base de travail commune (encore en évolution) sur les incidents cyber.

E. En France, la clarification de la couverture du GAREAT pour les cas de cyberterrorisme

Certains faits générateurs cyber peuvent constituer des actes de terrorisme.

En France, le Code pénal a pris acte d'une telle réalité en introduisant à l'article 421-1 *« les infractions en matière informatique définies par le livre III du présent code »* en tant qu'acte de terrorisme.

Pour être qualifiées comme tel, il faut que de telles infractions aient été commises « intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur ».

Pour la couverture de dommages matériels générés par un acte de terrorisme, le marché français a mis en place un pool de co-réassurance, le GAREAT.

(86) Cambridge Center for Risk Studies, Cyber Accumulation Risk *Management, Managing cyber insurance accumulation risk,* fev. 2016.
(87) CRO FORUM est un groupe réunissant les risk managers du marché de l'assurance.
(88) CRO Forum, *Concept Paper on a proposed categorisation methodology for cyber risk*, juin 2016, [https://www.thecroforum.org/wp-content/uploads/2016/06/ZRH-16-09033-P1_CRO_Forum_Cyber-Risk_web-2.pdf].

Focus – Le GAREAT

La loi du 9 septembre 1986 impose aux assureurs d'inclure une couverture terroriste dans les polices dommage. À la suite des attentats du 11 septembre 2001 aux États-Unis, et dans la crainte de nouveaux attentats sur le territoire français, un partenariat public-privé a donné naissance, dans un contexte d'effondrement des capacités de réassurance de marché, à un pool de co-réassurance avec une garantie illimitée de l'État portée par la Caisse centrale de réassurance (CCR) au-delà d'un certain seuil[89].

Le GAREAT est donc une structure de marché, créée fin 2001, en charge de la gestion de la réassurance des risques attentats et actes de terrorisme[90].

L'article L 126-2 du Code des assurances pose le principe de la garantie obligatoire des risques d'origine terroriste en matière d'assurance dommages. Toutefois, cette garantie ne couvre que les dommages matériels et les dommages immatériels consécutifs (comme la perte d'exploitation), subis en France par des biens situés sur le territoire national et couverts par un contrat d'assurance garantissant les dommages d'incendie, ainsi que pour les dommages aux corps de véhicules terrestres à moteur.

Le GAREAT est un pool de réassurance. Ses limites d'intervention ne sont opposables qu'aux assureurs adhérents, qui lui cèdent des risques. Les garanties accordées aux assurés sont, quant à elles, définies uniquement par leurs polices.

Le GAREAT intervient-il en cas de dommages générés par un acte de cyberterrorisme ?

Trois situations doivent être distinguées.

(89) AMRAE, Note technique GAREAT, [http://amrae.fr/sites/default/files/fichiers_upload/GAREAT%20Note%20technique_AMRAE.pdf].
(90) GAREAT, *Qui sommes-nous ?* [http://www.gareat.com], (consulté le 10 mai 2017).

– Le phénomène cyber génère un dommage direct.

Dans ce cadre, le GAREAT couvre ces dommages.

Exemple : un malware affecte le système de sécurité d'un process industriel, ce qui provoque un incendie et une perte d'exploitation.

– Le phénomène cyber génère une perte d'exploitation sans dommage direct.

Dans ce cadre, le GAREAT n'interviendra pas, même si le bien affecté par l'attaque est couvert en incendie.

Exemple : en cas d'attaque par déni de service (DDOS) impactant un réseau informatique, il y a potentiellement une perte d'exploitation et des frais exposés, mais pas de dommage matériel direct.

– Le phénomène cyber génère une atteinte aux données.

La situation est plus complexe en cas d'atteintes aux données. Lorsque l'accès illicite, la perte, le vol ou la corruption de données affectent un système d'information assuré en incendie, est-ce un dommage matériel cessible à GAREAT ou un pur dommage immatériel non cessible ?

Pour répondre à cette question, le GAREAT estime que le cadre fixé par l'article L. 126-2 impose d'aller au-delà de la seule perte de données et de s'intéresser au support d'information (hardware, mémoire, disque dur, clés USB…) sur lequel se trouvent ces données, et qui doit en premier lieu bénéficier d'une garantie incendie. Il identifie trois situations.

Si le support est irrémédiablement corrompu et techniquement irréparable : il y a atteinte à la structure du support assuré, qui subit bien un dommage matériel. Le GAREAT prend en charge le dommage au support et les frais consécutifs, dont les frais de restauration des données dans les conditions et les limites prévues par le contrat.

Si le support est techniquement réparable : la structure du support n'est pas atteinte ; il n'y a pas de dommage matériel. Les frais de remise en fonctionnement du support et de restauration des données affectées constituent un dommage immatériel non consécutif et ne seront pas pris en charge par le GAREAT.

En conséquence, le GAREAT a modifié son règlement intérieur à compter de 2017 et ainsi précisé les limites de sa couverture du cyberterrorisme en réécrivant son exclusion spécifique pour les conséquences des actes

cyberterroristes autres que les dommages matériels, les frais consécutifs et la perte d'exploitation consécutive légalement couverts par les assureurs conformément à l'article L. 126-2 du Code des assurances. Les articles 9 al. 3. et 14 al. 3 du règlement intérieur 2017 du GAREAT donnent une liste indicative des contrats et garanties exclus ou n'entrant pas dans le champ d'application de la section des grands risques et des risques petits et moyens. Sont notamment exclus :

« Les dommages immatériels non consécutifs causés par les actes de cyber terrorisme définis par les articles 421-1 2° et 323-1 à 323-8 du Code pénal, en particulier ceux causés par les logiciels malveillants, les virus et les cryptolockers, par le piratage et les attaques informatiques et attaques par déni de service, ainsi que par les vols de données. Sont ainsi exclues les conséquences de la seule atteinte aux données ou de leur perte ou de leur inaccessibilité, sans altération techniquement irréversible du support d'information. »

Ainsi, les contrats d'assurance cyber ne délivrant pas de garantie de dommages à la structure du support ne font pas l'objet de cession en réassurance auprès du pool GAREAT.

II. … qui appelle une réponse assurancielle adaptée

Aujourd'hui, pour tirer parti de ce nouveau contexte et accompagner au mieux les efforts du marché en faveur d'une réduction de la menace cyber, les pouvoirs publics et les investisseurs institutionnels ont un rôle à jouer.

Les plans d'investissement public français et européen devraient favoriser le développement d'une filière française et européenne d'excellence dans le domaine de la cyber-protection. Par ailleurs, les investisseurs institutionnels, dont les assureurs, pourront intégrer dans leurs politiques d'allocation d'actifs la nécessité de la réduction du risque cyber. Le soutien de projets de pointe dans la filière de la cyber-protection apparaîtrait particulièrement cohérent à cet égard.

Surtout, une évolution de l'offre d'assurance s'impose, afin de donner au marché de l'assurance cyber, en France notamment, une nouvelle

dynamique. Pour toutes les raisons évoquées dans le chapitre précédent, les projections d'évolution du marché de l'assurance cyber anticipent de fortes hausses des primes souscrites dans les prochaines années. Le marché de l'assurance cyber devrait doubler aux États-Unis[91] et tripler en Europe d'ici à 2018[92].

Cette croissance devra notamment aller de pair avec une clarification de l'offre cyber, un élargissement de l'offre de services dans l'accompagnement des assurés, et une optimisation de la tarification du risque et de la maîtrise des cumuls (qui impacte la souscription), que l'élargissement des bases de données statistiques devrait progressivement faciliter.

A. Clarifier l'étendue et l'articulation des couvertures

À mesure que les cyber-risques se sont développés, la question de savoir si les contrats « traditionnels » de dommages et de RC couvraient ces nouveaux risques, même s'ils ne les mentionnaient pas explicitement, est devenue de plus en plus cruciale : c'est la problématique dite des « silent cover ».

Le terme de « silent cover » renvoie à la couverture de faits générateurs d'origine cyber par des contrats traditionnels existants :

- sans que celle-ci ait été identifiée comme telle ;
- sans que celle-ci ait été prise en compte dans la tarification des contrats traditionnels par l'assureur.

La clarification des couvertures nécessite également un éclaircissement de l'articulation entre les contrats traditionnels et les contrats cyber dédiés. Pour les assureurs, il y a un double enjeu à clarifier l'étendue et l'articulation des couvertures cyber :

(91) PwC, *Insurance 2020 & beyond : Reaping the dividends of cyber resilience*, 2015.
(92) Insurance Information Institute, *Cyber risk : threat and opportunity, Insurance Information Institute, New York*, 2015.

- accompagner de nombreuses entreprises, TPE et PME notamment, que la complexité et l'opacité des couvertures cyber atomisées entre plusieurs types de contrats d'assurance dissuadent souvent de souscrire une assurance cyber (voir 1.III.B.) ;
- optimiser la quantification de leurs propres engagements et de leurs cumuls en levant l'incertitude liée aux « silent cover », qui sont appelées à être explicitées.

À ces différentes fins, et pour entamer une réflexion sur l'évolution à moyen et long terme des différents types de couvertures du risque cyber, plusieurs initiatives récentes ont entrepris d'analyser l'ensemble des couvertures pouvant être impactées à la suite d'une demande d'indemnisation. L'IRT system X[93], en partenariat avec la FFA (Fédération française de l'assurance), FERMA et l'AMRAE, a ainsi développé une matrice croisant les faits générateurs et les couvertures d'assurance cyber (traditionnelles ou cyber), afin d'avoir une meilleure visibilité sur l'articulation des garanties mobilisées pour couvrir ce risque. Ce travail met également en évidence les faits générateurs qui peuvent être couverts par différents types de polices, ainsi que les faits générateurs qui ne sont pas couverts par l'assurance.

Un travail au niveau du marché français est en train d'être réalisé sous l'égide de la FFA en vue de clarifier l'articulation des couvertures des différents contrats concernés (dommages aux biens, RC et cyber). Ce travail sur les « silent cover » permettra :

– aux assureurs et aux réassureurs de mieux gérer leurs cumuls d'engagements ;
– à leurs clients de mieux comprendre les différentes couvertures mobilisables pour couvrir ce risque.

À titre de comparaison, l'encadré suivant présente la façon dont le marché de Londres s'est saisi de ces différentes problématiques et a entrepris un travail de clarification du périmètre des couvertures cyber, à travers quatre initiatives.

(93) IRT System X, *La maîtrise du risque cyber sur l'ensemble de la chaîne de sa valeur et son transfert vers l'assurance,* 2016, [http://www.irt-systemx.fr/publications-archives/english-la-maitrise-du-risque-cyber-sur-lensemble-de-la-chaine-de-sa-valeur-et-son-transfert-vers-lassurance/]. Voir annexe (sur le site).

Focus – Définition et articulation des couvertures :
le cas anglo-saxon

I) La cyber stratégie du Lloyd's : surveillance de l'activité cyber des syndicats

Dès 2015, les Lloyd's ont mis en place une « Lloyd's Cyber-Attack Strategy[94] ». Cette stratégie a pour objectif de permettre un contrôle et une surveillance des syndicats britanniques d'assurance dans le cadre de leur activité de souscription d'assurance cyber.

Pour cela, il a été demandé aux syndicats, dans un premier temps, de détailler leur gestion du risque cyber, leur compréhension de ce risque et les éléments pris en compte lors de la souscription de couvertures et du calcul des primes associées.

Puis, dans un second temps, il leur a été demandé d'identifier leur niveau de risque et d'analyser les cumuls potentiels. Dans ce but, les syndicats doivent établir trois scénarios catastrophe plausibles de cyberattaques afin de calculer l'agrégation des expositions de leurs diverses couvertures en cas de réalisation d'un tel scénario.

Ces scénarios doivent également identifier les typologies de polices pouvant intervenir (polices traditionnelles et polices spécifiques) et les hypothèses de potentielles « silent cover ».

Ultimement, les syndicats doivent démontrer aux Lloyd's avant le 31 décembre 2017 qu'ils se sont saisis de la question et qu'ils ont mené des actions en conséquence.

(94) Lloyd's, *Cyber-Attack Strategy*, juin 2016.

II) L'action de l'autorité de régulation britannique

La « Prudential Regulatory Authority » (PRA) a également publié une consultation, en novembre 2016, invitant les assureurs à identifier, quantifier et manager les risques cyber couverts par leurs contrats[95]. Dans ce cadre, une lettre avait été adressée aux compagnies d'assurances afin de les sensibiliser à ce sujet[96]. Ces dernières avaient jusqu'au 14 février 2017 pour y répondre.

Le 5 juillet 2017, la PRA a publié un « supervisory statement[97] » reprenant les attentes de la PRA vis-à-vis des compagnies d'assurances à la suite des retours du marché britannique sur la consultation.

Les attentes de la PRA portent sur trois points.

Le « non-affirmative cyber-risk » (terme qui remplace les « silent risk »).

La PRA n'intervient pas dans la régulation du prix et du contenu des produits. Elle s'assure seulement de la maîtrise par les compagnies d'assurances du risque qu'elles couvrent et de la suffisance des réserves et fonds propres afin de garantir leur solvabilité.

Pour cela, elles doivent identifier les couvertures par lesquelles le risque cyber peut être couvert. Il est attendu qu'elles ajustent leurs primes en conséquence, qu'elles introduisent des exclusions fermes et des limites de couvertures associées.

En l'absence d'exclusion, pour les compagnies qui n'auraient pas ajusté volontairement leurs primes, la PRA vérifiera qu'une telle action a été validée par les instances dirigeantes de la compagnie. Les contrats devront être re-rédigés afin d'identifier clairement que la couverture du risque cyber est comprise dans le produit.

(95) PRA, Cyber insurance underwriting risk, consultation paper, CP39/13, nov. 2016. [http://www.bankofengland.co.uk/pra/Documents/publications/cp/2016/cp3916.pdf].
(96) PRA, Letter Cyber underwriting risk, 14 nov. 2016 -http://www.bankofengland.co.uk/pra/Documents/about/letter141116.pdf.
(97) PRA, Cyber insurance underwriting risk, supervisory statement, SS4/17, juil. 2017, [http://www.bankofengland.co.uk/pra/Documents/publications/ss/2017/ss417.pdf].

La stratégie en matière de cyber-risque et l'appétit du risque

Les entreprises doivent définir une cyber-stratégie claire et approuvée par les instances dirigeantes. Cette stratégie comprend l'articulation des différents engagements, la prise en compte des couvertures silencieuses, l'identification des secteurs concernés par les couvertures, l'agrégation des limites… Cette stratégie doit inclure également des stress-tests afin d'identifier les potentielles agrégations de risques.

La cyber-expertise

Il s'agit de maîtriser l'évolution constante de l'environnement cyber et de démontrer un engagement à suivre l'évolution du risque cyber couvert par les contrats d'assurance.

III) Un exemple de clause mise à disposition du marché : la clause d'exclusion du risque cyber en assurance maritime du marché de Londres

Au début des années 2000, le marché de Londres de l'assurance transport a mené des travaux pour prendre en compte le risque cyber en proposant un modèle de clause type qui soit partagé par l'ensemble du marché. Aujourd'hui, le marché international de l'assurance transport, et plus particulièrement maritime, est majoritairement dans une logique d'exclusion du risque cyber. À cet effet, un modèle de clause est notamment utilisé afin d'exclure la couverture du risque cyber d'origine malveillante par les contrats de dommages et de responsabilité. Il s'agit de la clause d'exclusion générale CL 380. Elle ne s'applique pas en cas de faits générateurs cyber résultant d'une erreur humaine ou d'un dysfonctionnement.

Cette approche d'une clause type d'exclusion mise à disposition du marché de l'assurance transport maritime a le mérite de la clarté pour les assureurs comme pour les assurés, et lève toute équivoque sur la couverture du risque cyber.

Cette clause reste à la libre discussion des parties.

Clause d'exclusion des risques cybernétiques

[traduction libre de la clause CL 380 (10/11/2003)]

« 1.1 Sous réserve des dispositions de l'article 1.2 ci-dessous, sont exclus les pertes et dommages, recours de tiers ou dépenses résultant directement ou indirectement de l'utilisation ou l'exploitation, avec l'intention de causer des dommages, de tout ordinateur ou équipement informatique, programme ou logiciel informatique, virus informatique, code falsifié ou transmission de données, ou tout autre système électronique.

1.2 Si la présente clause fait l'objet d'un avenant à des polices couvrant les risques de guerre, guerre civile, révolution, émeute, insurrection, ou conflits en résultant, ou tout acte d'hostilité effectué par ou contre une puissance belligérante, acte de terrorisme ou toute action menée par des personnes agissant pour un motif politique, l'article 1.1 ne pourra pas exclure les pertes – dans la mesure où elles sont couvertes – résultant de l'utilisation de tout ordinateur, équipement informatique ou programme ou logiciel informatique, ou de tout autre dispositif électronique installé dans le système de lancement et/ou de guidage, et/ou dans le mécanisme de mise à feu de toute arme ou de tout missile. »

IV) Une nouvelle initiative du marché de Londres en matière d'assurance aviation portée par l'Aviation Insurance Close Group (AICG)

Ce groupe de travail, qui émane du marché de Londres, est en train de réfléchir à l'introduction d'une clause d'exclusion similaire à celle qui est proposée en matière de transport maritime.

B. Améliorer l'accompagnement de l'entreprise

Dans un nouveau contexte de risque et de contraintes réglementaires, les assureurs sont appelés à assumer, en plus de la couverture d'assurance des incidents cyber, un rôle élargi d'accompagnement des entreprises. Il comprend, dans le cadre du processus de souscription :

- l'information sur les développements de la menace et la veille juridique – d'autant plus crucial que les assureurs sont un relais essentiel d'informations sur l'évolution juridique auprès de leurs clients et prospects ;
- l'analyse de risque et le conseil en prévention et mitigation des risques afin de réduire la vulnérabilité aux incidents cyber pendant la période de couverture ;
- le suivi de la gestion de crise et l'analyse de ses impacts financiers et opérationnels afin de réduire l'impact des incidents cyber (à cet égard, les cyberattaques, et notamment les rançongiciels, nécessitent des temps de réactivité extrêmement courts ; en raison de la paralysie de leur système d'exploitation, les entreprises ont impérativement besoin d'une réponse quasiment instantanée de la part de leurs prestataires de services ; la maîtrise technique sera d'autant plus importante lors de sinistres de masse qui nécessiteront la mobilisation par les compagnies d'assurances de nombreux experts spécialisés en cyber-risque).

Ces fonctions élargies appellent une montée en compétences d'experts cyber tant en souscription qu'en gestion de sinistre. Une enquête récente menée par Verisk Analytics souligne toutefois que plus de la moitié des assureurs n'ont pas de souscripteurs dédiés au cyber-risque et font appel à des spécialistes d'autres lignes d'assurances pour gérer les polices cyber[98].

(98) Cité dans Oleg Bogomolniy, *Cyber Insurance Conundrum : Using CIS Critical Security Controls for Underwriting Cyber Risk,* publishes by The SANS Institute, 2017, p. 14.

Les compagnies d'assurances doivent donc, de façon urgente, développer la spécialisation de leurs personnels, notamment en les incitant à passer le Certificat Digital Assurance pour faire valider leurs compétences en matière de risque cyber.

C. Affiner la segmentation des risques

L'expérience accumulée par les assureurs leur permettra de quantifier de plus en plus précisément l'exposition réelle des assurés au cyber-risque et, consécutivement, d'établir une discrimination des risques et une segmentation de leurs tarifs plus pertinentes.

La formation d'experts cyber chez les assureurs et chez les assurés, les partenariats noués avec des pourvoyeurs de services en cybersécurité, les efforts en cours pour adopter des définitions de risques harmonisées et rassembler des données sur les incidents cyber passés à l'échelle du marché afin d'enrichir les bases statistiques devraient contribuer à cette évolution.

Une approche tarifaire plus apte à refléter l'exposition réelle des assurés au cyber-risque permettra de développer une plus grande appétence de couverture pour les meilleurs risques.

D. Trancher la question de l'assurabilité des sanctions administratives et des rançons

Le Code des assurances français n'évoque pas la question de l'assurabilité des sanctions ou des rançons.

1. La question ouverte des sanctions administratives

En France, la CNIL dispose d'un pouvoir de sanction administrative à l'égard des entreprises en cas de violation des règles de sécurité relatives aux données, depuis la modification de la loi informatique et libertés de 1978 en 2004[99]. Ce pouvoir a été renforcé au niveau national par la loi

(99) *Loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés,* art. 45.

Lemaire du 7 octobre 2016, et également par le règlement européen relatif à la protection des données personnelles (RGPD), qui sera applicable dans l'ensemble des États membres le 25 mai 2018[100].

La question de l'assurabilité des sanctions administratives en cas de violation de la réglementation sur la protection des données à caractère personnel se pose. Cette interrogation est d'autant plus importante que les sanctions administratives encourues sont très lourdes (et le seront plus encore lorsque le RGPD sera applicable).

Il n'y a pas d'unanimité sur la réponse à apporter à cette question. Certains considèrent que l'assurance est nécessairement illicite par analogie avec les sanctions pénales, car contraire à l'ordre public. En effet, la cour d'appel de Paris, dans un arrêt du 14 février 2012[101], a jugé qu'une sanction prononcée par l'Autorité des marchés financiers (AMF) n'était pas assurable au visa de l'article 6 du Code civil selon lequel *« on ne peut déroger, par des conventions particulières, aux lois qui intéressent l'ordre public et les bonnes mœurs »*.

Cet arrêt de la cour d'appel soutient que l'assurabilité des sanctions administratives prononcées par l'AMF est contraire à l'ordre public, car elle les priverait de leur caractère dissuasif.

À l'inverse, un arrêt de la Cour de cassation du 14 juin 2012[102] laisse place au doute. En l'espèce, un dirigeant social avait été condamné par l'AMF à une amende. Il entendait se prévaloir de son assurance « Responsabilité des dirigeants », laquelle couvrait toutes les amendes et/ou pénalités civiles. La Cour de cassation ne se prononce pas sur l'assurabilité de ce risque, mais neutralise le jeu de l'assurance au seul motif que l'assuré avait commis une faute intentionnelle incompatible avec l'aléa.

Il résulte de cet arrêt une certitude et une interrogation.

(100) E. GABRIE, « Les pouvoirs des autorités de protection des données », *Dalloz IP/IT*, 2017, P. 268 ; *loi no 2016-1321 du 7 octobre 2016 Loi pour une République numérique* ; règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.
(101) CA Paris, Pôle 02 ch. 05, 14 fév. 2012, no 09/06711.
(102) Cass. civ. 2e, 14 juin 2012, pourvoi no 11-17.367.

Une certitude : la Cour de cassation ne se prononce pas sur la validité de l'assurance, alors même qu'elle en aurait eu la possibilité, dès lors que l'ordre public était en jeu.

Une interrogation : le silence gardé sur la validité de la clause et le débat mené exclusivement sur le caractère intentionnel de la faute de l'assuré signifie-t-il que la Cour de cassation juge assurable le risque de condamnation de l'AMF ?

La doctrine est partagée, certains auteurs se prononçant en faveur d'une nullité de la stipulation, d'autres estimant, *a contrario*, qu'il est permis de s'assurer contre un tel risque, pourvu que la faute couverte ne soit pas intentionnelle[103].

Cela posé, à supposer cette interprétation valide, une autre difficulté se ferait jour.

Dans la mesure où certaines sanctions de la CNIL ne sont pas prononcées sans que la personne morale soit préalablement mise en demeure de se mettre en conformité, l'absence de mise en conformité par le responsable de traitement ne pourrait-elle pas être considérée comme un fait intentionnel, et donc exclure la question de l'assurabilité de cette sanction ?

Cette analyse doit être nuancée au regard de la loi du 7 octobre 2016, qui prévoit désormais la possibilité pour la CNIL d'exercer son pouvoir de sanction sans mise en demeure préalable. Ainsi, la question de la faute intentionnelle post-mise en demeure ne se pose pas dans cette situation. D'ailleurs, la CNIL a déjà appliqué ce nouveau régime dans la décision « Hertz » du 18 juillet 2017 en infligeant une amende de 40 000 € à l'encontre du responsable de traitement[104] pour négligence, après qu'un grand nombre de données de ses clients ont été rendues accessibles au public, du fait d'un changement de serveur de son sous-traitant.

(103) RTD Com.2012 p 813, Nicolas Rontchevsky ; Bulletin Joly Sociétés 01/10/2012 no 10 – page 696 par Bernard Saintourens.
(104) Délibération de la formation restreinte no SAN-2017-010 du 18 juillet 2017 prononçant une sanction pécuniaire à l'encontre de la société HERTZ FRANCE.

Enfin, certaines compagnies d'assurances semblent avoir développé une pratique consistant à indemniser les sanctions pécuniaires administratives « sous condition d'assurabilité ». Par nature, il est difficile d'identifier ce qui est « assurable[105] ». Cette absence de précision peut s'expliquer par l'absence même de solution stable prévue par la loi ou fixée par la jurisprudence. C'est par une rédaction en retenue des clauses de garantie que ces compagnies ouvrent la possibilité d'une indemnisation, comme l'indique la rédaction suivante.

« Amendes et pénalités : le cas échéant, et par dérogation partielle à l'exclusion générale de garantie no XX ci-après, les amendes et pénalités qui vous auraient été imposées dans le cadre des enquêtes et actions visées ci-dessous, dès lors qu'elles sont légalement assurables au regard du droit applicable[106]*. »*

L'absence de consensus sur ce sujet met en exergue le besoin de préciser officiellement la législation pour, d'une part, clarifier les risques non transférables / non assurables portés par les entreprises et, d'autre part, éviter les différences d'interprétation de la loi entre professionnels de l'assurance.

Focus – Projet de réforme de la responsabilité civile et inassurabilité des amendes civiles

Dans le projet de réforme de la responsabilité civile[107], le projet d'article 1266-1 du Code civil prévoit que l'auteur d'un dommage qui a délibérément commis une faute en vue d'obtenir un gain ou une économie peut être condamné par le juge à la demande de la victime ou du ministère public, et par une décision spécialement motivée, au paiement d'une amende civile. Elle n'est pas assurable.

(105) HELENON Nicolas, HESLAUT Clarisse, « Données personnelles – Sur l'assurabilité des sanctions administratives », *Expertises*, mai 2017, no 424.
(106) Idem.
(107) Ministère de la Justice, projet de réforme de la responsabilité civile, mars 2017, [http://www.justice.gouv.fr/publication/Projet_de_reforme_de_la_responsabilite_civile_13032017.pdf].

2. Les rançons

Une nouvelle forme de cybercriminalité s'est rapidement répandue : le « rançongiciel » (ou « ransomware » en anglais), un logiciel malveillant qui chiffre les données et réclame le paiement d'une somme, ou « rançon », pour que son propriétaire puisse les récupérer. Il se propage, par exemple, par courrier électronique à l'ouverture d'un lien ou d'une pièce jointe. Les données du système infecté sont alors « prises en otage » par le pirate, qui demande le paiement d'une rançon en échange de la restitution des données.

Deux hypothèses peuvent être envisagées pour récupérer les données devenues inaccessibles.

- Le recours à un expert informatique, qui peut intervenir pour tenter de restaurer les sauvegardes des données « prises en otage » par le cyberattaquant. Ces frais peuvent être pris en charge dans le cadre d'un contrat d'assurance.
- Le paiement de la rançon, qui ne permet pas forcément le déchiffrement des données (à titre d'exemple, le rançongiciel « NotPetya » était un virus qui ne permettait pas la récupération des clés de décryptage et donc des données) ; son assurabilité est sujette à discussion.

Sur le marché français, certains prônent l'inassurabilité de telles rançons pour des raisons d'ordre public. En effet, au motif que les fonds obtenus via ces agissements pourraient financer des actes terroristes, il est possible d'avancer que toute clause contractuelle prévoyant l'assurance de ces rançons serait nulle en vertu des dispositions des articles 6 et 1102 alinéa 2 du Code civil et 421-2-2 du Code pénal, car contraire à l'ordre public. Cette position semble commune à la majorité des pays de l'Union européenne, à l'exception, notamment, des Pays-Bas, du Royaume-Uni (depuis 1981 avec l'abrogation du « Ransom Act of 1782 ») ou de la Suisse, qui admettent l'assurance des risques criminels.

D'autres compagnies les garantissent, par analogie avec les contrats « kidnapping et rançon » (de l'anglais « kidnap and ransom »), qui, eux, interviennent à titre principal lorsque des vies humaines sont en jeu et prévoient des garanties complémentaires en matière de cyber-extorsion.

Focus – Position du ministère des Finances sur l'assurabilité des rançons à des entités terroristes

Une position officielle a été prise par la direction générale du Trésor[108] pour interdire *« les contrats d'assurance, dont l'objet est de garantir le paiement d'une rançon à Daech, comme à toute entité terroriste »*, *et pour encourager « l'insertion de clauses dans les contrats d'assurance "kidnapping et rançon" excluant le remboursement ou le paiement d'une rançon, directement ou indirectement, via des intermédiaires, qui bénéficieraient à Daech »*.

Ce communiqué se fonde sur l'article 421-2-2 du Code pénal qui qualifie d'acte de terrorisme « *le fait de financer une entreprise terroriste en fournissant, en réunissant ou en gérant des fonds, des valeurs ou des biens quelconques, ou en donnant des conseils à cette fin, dans l'intention de voir ces fonds, valeurs ou biens utilisés, ou en sachant qu'ils sont destinés à être utilisés, en tout ou partie, en vue de commettre l'un quelconque des actes de terrorisme prévus au présent chapitre, indépendamment de la survenance éventuelle d'un tel acte* » et sur le règlement (UE) 881/2002 selon lequel *« les fonds comprennent les garanties ; aucun fonds ni ressources économiques ne doivent être mis à disposition, directement ou indirectement, de terroristes désignés par ce règlement ; il est interdit de participer, sciemment ou volontairement, aux activités ayant pour objet ou pour effet, direct ou indirect, de contourner cette interdiction »*.

En matière cyber, il est souvent difficile de connaître l'auteur d'un acte et d'identifier l'origine terroriste ou non d'un incident.

Sauf à pouvoir démontrer qu'un piratage a été réalisé par une organisation terroriste, il demeure un vide juridique quant à la légalité de l'assurabilité des rançons.

(108) Communiqué du ministère des Finances, Disposition de vigilance financière à l'encontre de Daech, décembre 2015, [http://www.tresor.economie.gouv.fr/10858_lutte-contre-le-financement-de-daech].

Pour autant, comme en matière de sanctions administratives, certaines compagnies d'assurances tendent à couvrir les risques liés aux ransomwares dans des conditions définies par le contrat, à défaut de législation précise. L'analyse de tels contrats est rendue difficile par la clause de confidentialité qu'ils comportent. En effet, en matière de rançon, tant pour les personnes physiques que pour les données informatiques, la connaissance par les ravisseurs ou cyberattaquants potentiels d'une telle assurance transforme les assurés en cibles privilégiées.

E. Maîtriser le cumul des engagements

« En l'absence de contrôles effectifs du risque de cumul, un (ré)assureur pourrait se retrouver avec des pertes catastrophiques qui épuiseraient son capital et diminueraient sa capacité à respecter ses engagements à l'égard des preneurs d'assurance[109]. » De plus en plus d'observateurs, à l'instar de l'auteur de la dernière étude de Swiss Re sur ce sujet, mettent en exergue le risque de cumul très spécifique que la souscription de cyber-risques fait peser sur le bilan des (ré)assureurs. « Les souscripteurs s'inquiètent de leur exposition à une violation [de données personnelles] qui affecterait un grand nombre de leurs assurés simultanément. »

Pour les assureurs, l'éventualité de devoir indemniser de très nombreux assurés pour un même fait générateur cyber est forte, principalement pour les raisons suivantes[110].

- Les interconnexions de plus en plus nombreuses entre les systèmes d'information entraînent des effets dominos en cas, par exemple, de contamination par un virus informatique.
- Au niveau mondial, l'utilisation des mêmes composants informatiques (logiciels, ordinateurs, serveurs, systèmes, routeurs…), des mêmes services (cloud, infogérance), des mêmes objets connectés, entraîne une aggravation des risques. Une vulnérabilité chez l'un de ces prestataires pourra entraîner un sinistre sériel de grande ampleur.

(109) Swiss re, *Cyber : comment venir à bout d'un risque complexe ?*, 2017, no 1, p. 21.
(110) Cf. Partie 1, I, B.

- L'absence de contrainte géographique à la propagation d'un incident cyber : la propagation du virus WannaCry, qui s'est répandu en utilisant les versions antérieures du système d'exploitation Windows 10, pour lesquelles les mises à jour de sécurité n'avaient pas été effectuées, illustre ce phénomène.
- Les cumuls de garanties : les polices traditionnelles de dommages aux biens et de responsabilité civile peuvent intervenir en plus des couvertures spécifiques cyber, entraînant un risque d'arbitrage délicat selon les niveaux de franchise, les montants de garantie (avec plafond annuel ou par sinistre) et les modalités de gestion de sinistre.

Ainsi, un même événement cyber est susceptible de causer de multiples sinistres au titre de diverses polices chez de multiples assurés à travers le monde[111]. Ce risque d'indemnisation simultanée au titre de différents contrats est un frein à la mobilisation de capitaux suffisants pour les besoins du marché. Un travail de clarification des garanties et exclusions couvrant les risques cyber permettrait d'avoir une meilleure compréhension des engagements et une meilleure connaissance des cumuls d'engagement.

Pour les réassureurs, les risques de cumuls sont encore amplifiés.

- Une entreprise étant couverte par plusieurs assureurs, un même incident cyber sur cette entreprise peut déclencher des sinistres au titre de plusieurs contrats de réassurance.
- Un incident cyber chez un assuré peut être indemnisé au titre de plusieurs contrats d'assurance. Ces mêmes contrats peuvent être cédés à travers différents contrats de réassurance.
- En cas de catastrophe cyber de grande ampleur, la manière dont répondraient les contrats de réassurance classiques (responsabilité civile générale ou professionnelle, dommages…) reste incertaine.

Pour parer au risque de cumul, les (ré)assureurs recueillent un maximum d'informations sur de potentielles vulnérabilités communes (identification des fournisseurs de services en nuage et des logiciels utilisés notamment)

(111) Cf. Partie 2, I, A. Clarifier l'articulation des couvertures.

afin d'établir une cartographie du risque potentiel d'accumulation et d'établir des indicateurs d'impact de l'interruption de l'activité du fournisseur de services Internet, fournisseur de services cloud ou fournisseur de services de paiement, par exemple.

L'une des solutions pour appréhender au mieux ces phénomènes de cumul est l'élaboration de scénarios cyber-catastrophiques.

Ces scénarios devront répondre à plusieurs exigences : être de grande ampleur tout en restant probables (éviter les scénarios « fin du monde ») et permettre d'estimer un impact financier aussi bien général (impact sur l'économie) que sur les réassureurs.

Les scénarios réalisés par les grandes entreprises assurées viendront nourrir ceux des assureurs et réassureurs.

Les régulateurs comme les agences de notation – qui ont fait savoir depuis 2015-2016 qu'une accumulation mal contrôlée de risques cyber pourrait affecter négativement la notation des (ré)assureurs – sont particulièrement vigilants quant à la bonne gestion des cumuls.

F. La part croissante des actifs intangibles, un défi pour les assureurs

La réputation, la propriété intellectuelle ou la perte d'opportunités sont des actifs intangibles très exposés au risque cyber. Dans une économie de plus en plus numérisée, leur poids dans la valorisation des entreprises a considérablement progressé.

Focus – Comptabilisation et évaluation des actifs intangibles

Plus de 50 % de la valeur de l'entreprise est représentée par des actifs intangibles (valeur de la marque, valeur des brevets, valeur de la technologie, valeur du système d'information, valeur des équipes constituées…), alors que moins de 20 % de ces actifs seraient comptabilisés[112].

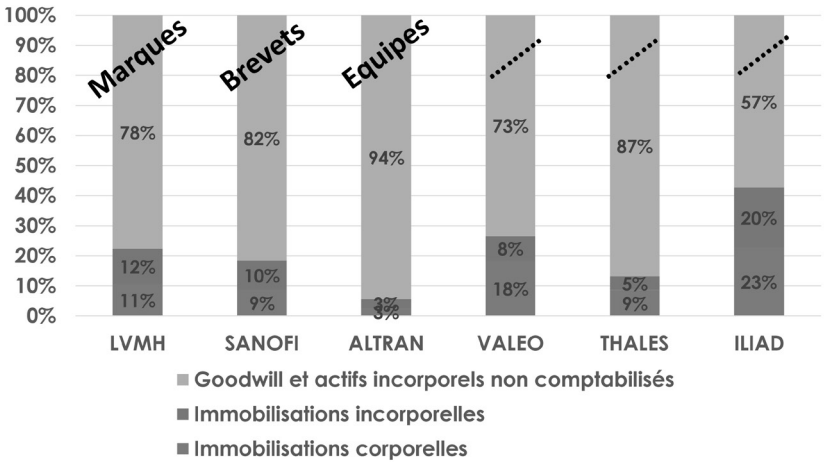


Illustration à partir de la capitalisation boursière d'entreprises cotées françaises

En cas d'incident cyber, les actifs intangibles représentent désormais une part importante des pertes potentielles.

Le marché n'est aujourd'hui pas en mesure d'assurer ce type d'actifs de manière standardisée.

(112) E. CHASTENET, Comptabilisation et évaluation des actifs intangibles, généralités – Le cas des marques, Présentation réalisée lors de la réunion de l'IRT System X du 18 avril 2017.

Cette demande émane principalement des grandes entreprises. Cette problématique de l'assurance des biens intangibles n'est pas nouvelle et dépasse la question des risques cyber. Pour couvrir ces biens, la réponse assurantielle n'est pas à ce jour la plus adaptée, en raison notamment de la difficulté de quantifier l'actif et de mesurer le risque. Des solutions alternatives peuvent exister pour les grands comptes.

Les conditions de transfert de ces risques à l'assurance et à la réassurance demeurent donc à ce jour un sujet d'étude.

PARTIE 3
Dix préconisations pour mieux assurer le risque cyber

Les préconisations suivantes visent l'assurance cyber des entreprises, et plus particulièrement des TPE/PME et des collectivités locales. Le transfert du risque cyber vers l'assureur doit s'intégrer dans une stratégie globale de gestion financière du risque cyber et être précédé par l'évaluation du risque, sa prévention (thème qui fera l'objet d'un autre cahier de cette commission) et l'anticipation de la gestion de crise.

Préconisations à l'attention des assureurs et des gestionnaires de risque

Préconisation 1 : accélérer le développement d'une culture du risque cyber

1) **Informer** les entreprises assurées **sur les risques induits par l'usage des nouvelles technologies de l'information et de la communication ;** les **sensibiliser** aux **obligations réglementaires nationales** et européennes en les invitant notamment à consulter régulièrement le nouveau site Cybermalveillance.gouv.fr, ainsi que les sites de l'ANSSI et de la CNIL.

2) Développer des partenariats avec les représentants des acteurs économiques (fédérations professionnelles, syndicats et associations professionnels, regroupements de collectivités) dans le cadre du nouveau dispositif national d'assistance aux victimes (le groupement d'intérêt public ACYMA), afin qu'ils **informent leurs membres de la possibilité de transfert du risque cyber vers l'assurance.**

3) Inciter les salariés des entreprises d'assurances à faire valider le plus rapidement possible leurs compétences en matière de risque cyber en passant le **Certificat Digital Assurance.**

Préconisation 2 : expliquer clairement les contenus des différentes couvertures cyber et faciliter la comparaison des offres d'assurance

Proposer aux entreprises, lors de la souscription ou du renouvellement d'un contrat d'assurance, un **audit de leur couverture d'assurance contre les risques cyber** afin de mettre en évidence l'étendue de leur couverture, de clarifier l'articulation des couvertures cyber offertes par les différentes polices déjà souscrites (polices dommage/responsabilité civile/fraude ou polices dédiées au risque cyber) et d'identifier d'éventuelles redondances et/ou failles de couverture.

Établir et mettre régulièrement à jour une **liste d'éléments essentiels du contrat d'assurance cyber** (relatifs à la territorialité, à l'étendue des garanties, aux services associés et exclusions, etc.), qui permettra aux entreprises de mieux appréhender l'offre d'assurance et sa pertinence au regard de leur exposition au risque. Un groupe d'experts rassemblant des assureurs et des spécialistes de la gestion de risques sera constitué à cette fin.

Préconisation 3 : renforcer la relation de confiance entre assureurs et assurés dans la gestion des contrats cyber

Rédiger une **charte type** engageant l'assureur (et autres prestataires associés) à respecter la confidentialité et la sécurité des informations partagées par l'assuré à la souscription du contrat et lors de la gestion d'un sinistre.

Ce travail sera entrepris sous l'égide de la FFA et avec le concours de l'ANSSI, de l'AMRAE et de tout autre acteur pertinent.

Préconisations à l'attention des assureurs et réassureurs, de l'ANSSI et de la CNIL

Préconisation 4 : développer un cadre de sécurité numérique pour les TPE/PME

Développer un cadre de sécurité numérique pour les TPE/PME qui s'adapte à leur taille et à leur secteur d'activité en s'appuyant sur les normes développées par l'ANSSI pour les grandes entreprises et les OIV.

Les assureurs encourageront le respect de ces normes.

Préconisation 5 : mutualiser les données résultant d'incidents cyber

Définir les **modalités d'un partage des informations relatives aux incidents de sécurité des systèmes d'information ou de violation de données** grâce à une coopération de l'ANSSI, du GIP ACYMA, de la CNIL et de la FFA.

Ce partage d'informations pourra se faire sur la base des travaux déjà réalisés au niveau international, notamment par le CRO Forum[113]. Il permettra la constitution d'une base de données qualitatives et quantitatives sur les incidents cyber (et les montants des indemnisations afférentes), en vue d'en améliorer la gestion financière.

(113) The CRO Forum is a group of Chief Risk Officers from large multi-national insurance companies that focuses on developing and promoting industry best practices in risk management (see https://www.thecroforum.org).

Préconisation 6 : piloter les expositions et les cumuls de risques des assureurs et réassureurs

Élaborer des scénarios de catastrophes cyber afin de renforcer la résilience de l'économie nationale face à ce type d'événement en invitant les principaux acteurs du marché de l'assurance et de la réassurance à coopérer avec l'ANSSI.

Préconisations à l'attention des instances européennes

Préconisation 7 : définir au niveau européen un ensemble de normes techniques facilitant l'évaluation du niveau de sécurité cyber des assurés

Élaborer un cadre de certification du niveau de sécurité des logiciels et produits techniques qui permettrait de créer un **label européen de cybersécurité** pour les acteurs du monde numérique[114].

Préconisation 8 : établir les conditions d'une concurrence équitable entre les assureurs cyber

Inviter les autorités réglementaires de l'Union européenne à adopter un cadre juridique permettant un traitement harmonisé de la question de l'assurabilité des rançons au sein du marché européen.

(114) Proposition de Règlement sur l'agence européenne de cyber-sécurité (ENISA) et son annexe - France 24, Une agence et un label de l'UE pour affronter les cybermenaces, 19 sept. 2017, [http://www.france24.com/fr/20170919-une-agence-label-lue-affronter-cybermenaces].

Préconisation 9 : mettre en place, au niveau européen et international, une veille réglementaire et un suivi de l'évolution des marchés

Développer, à l'initiative des instances européennes, une plate-forme en ligne présentant de façon succincte les **informations réglementaires et de marché sur la gestion du risque cyber**[115] dans les principaux pays de l'OCDE, en coopération avec les organisations internationales pertinentes.

Cette plate-forme rendra notamment compte des initiatives nationales et internationales publiques et privées relatives au développement du marché de l'assurance cyber.

(115) Cette plate-forme pourra s'inspirer du rapport de l'OCDE intitulé : *Enhancing the role of insurance in cyber risk management,* 2017.

Préconisation à l'attention des pouvoirs publics et des investisseurs français et européens

Préconisation 10 : orienter l'investissement public et privé vers l'émergence d'une filière française et européenne d'excellence en cyber-technologie

Un effort d'investissement des pouvoirs publics et des choix cohérents de la part des investisseurs institutionnels devraient accompagner le développement du marché de l'assurance cyber.

Les plans d'investissement public français et européen devraient favoriser le développement d'une filière française et européenne d'excellence dans le domaine de la cyber-protection et accompagner les efforts du marché en faveur d'une réduction de la menace cyber.

En tant qu'investisseurs institutionnels, les assureurs pourront également intégrer dans leurs politiques d'allocation d'actifs la nécessité de la réduction du risque cyber, notamment en soutenant des projets de pointe dans la filière de cyber-protection.