MINISTÈRE
DE L'ÉCONOMIE,
DES FINANCES
ET DE LA SOUVERAINETÉ
INDUSTRIELLE ET NUMÉRIQUE

Liberté
Égalité
Fraternité

Direction générale
du Trésor

Le développement de l'assurance du risque cyber

Septembre 2022

Édito du directeur général du Trésor **4**

Synthèse **5**

Synthèse des recommandations **7**

I. Malgré la multiplication des cyberattaques, le marché de l'assurance du risque cyber reste insuffisamment structuré pour se développer **9**

1.1. Alors que le coût croissant des cyberattaques crée un besoin de couverture du risque par les assureurs, le marché de l'assurance du risque cyber peine à émerger 9

1.1.1 La numérisation de l'économie conduit à une multiplication des cyberattaques de plus en plus coûteuses 9

1.1.2 Pourtant, le marché de l'assurance du risque cyber demeure un marché de niche en France. 11

1.2 Le marché de l'assurance du risque cyber peine à se développer en France, notamment en raison d'une insuffisante structuration du marché 14

1.2.1 Les incertitudes entourant le cadre juridique constituent un obstacle à la constitution d'un marché de l'assurance du risque cyber 14

1.2.2 Les difficultés à mesurer le risque cyber entravent la définition d'une offre cyber 19

1.2.3 Dans un contexte de contraction des capacités assurantielles et ré-assurantielles, les caractéristiques du risque cyber limitent les possibilités de couverture 20

1.2.4 La sous-estimation du risque cyber et l'accompagnement encore insuffisant des entreprises réduisent la demande d'assurance du risque cyber 23

II. Le développement de l'assurance du risque cyber passe par une clarification de son cadre juridique, l'adoption d'outils et de pratiques visant à mieux le mesurer et le partager ainsi que par des efforts accrus de sensibilisation et d'accompagnement des entreprises **26**

2.1. La clarification du cadre juridique faciliterait la constitution d'un marché de l'assurance du risque cyber 26

2.1.1 L'adoption de bonnes pratiques de rédaction des contrats voire une obligation renforcée d'information permettraient de clarifier l'étendue des garanties cyber 26

2.1.2. L'assurabilité des cyber-rançons pourrait être conditionnée au dépôt de plainte afin de renforcer la lutte contre ces pratiques tout en permettant une indemnisation des victimes 28

2.1.3 Afin de clarifier le cadre juridique, l'inassurabilité des sanctions administratives pourrait être expressément mentionnée dans le code des assurances 29

2.1.4 Il est recommandé de poursuivre les travaux autour d'une potentielle exclusion de garantie pour cause de cyberguerre dans la mesure où une évolution législative apparaît prématurée 30

2.2. Une meilleure prise en compte du risque cyber dans le pilotage de l'activité assurantielle ainsi qu'un partage de données accru faciliteraient la mesure du risque 31

2.2.1. Améliorer la prise en compte du risque cyber dans le pilotage de l'activité assurantielle. 31

2.2.2 Répondre à la problématique du manque de données cyber 34

2.3. Un partage du risque plus efficace, impliquant des efforts de résilience accrus des entreprises et l'adoption de méthodes actuarielles innovantes, permettrait de viabiliser l'offre d'assurance du risque cyber 38

2.3.1. Face à la réduction des couvertures, la promotion de l'auto-assurance par la constitution de captives de réassurance peut constituer une solution pour les entreprises confrontées au risque cyber 38

2.3.2 L'adoption de pratiques innovantes par les assureurs, comme l'assurance paramétrique, pourrait faciliter la couverture du risque cyber 39

2.4. Un accroissement des efforts de sensibilisation des entreprises et un accompagnement renforcé stimulerait la demande d'assurance du risque cyber 41

2.4.1. Des efforts de sensibilisation accrus pour les entreprises, en particulier à destination des TPE/PME, pourraient réduire la sous-estimation du risque cyber 41

2.4.2. Le développement de l'offre de formation à la gestion du risque cyber pour les assurances et les réseaux de distribution est de nature à améliorer la qualité de l'accompagnement des entreprises 43

2.4.3. Une *task force* de l'assurance du risque cyber, qui pourrait être adossée à Paris Europlace, permettrait de piloter la mise en œuvre des recommandations et faire de la place de paris un pôle d'expertise cyber 43

Annexes : 45

Tableau des recommandations 45

Membres du groupe de travail 46

Contributeurs extérieurs 47

Édito du directeur général du Trésor

Ce rapport sur le développement de l'assurance cyber constitue l'aboutissement d'une année de réflexion au sein du groupe de travail dédiée à l'assurance du risque cyber. Depuis le 30 juin 2021, les services de la direction générale du Trésor, les représentants des assureurs et des entreprises, l'ACPR, l'ANSSI mais aussi des entreprises d'assurance et de réassurance, des distributeurs d'assurance, des actuaires et des experts du monde académique ont pu échanger et partager leurs contributions autour des enjeux de l'assurance du risque cyber. Cette concertation avec l'ensemble des acteurs du secteur a permis de dresser un constat partagé sur la situation du marché de l'assurance du risque cyber et, surtout, de dégager des pistes d'actions crédibles pour le développer.

La résilience face au risque cyber est aujourd'hui un enjeu majeur de souveraineté. Dans une période où les cyberattaques se multiplient, il s'agit d'une menace réelle pour la viabilité de nombreuses entreprises françaises. L'assurance a donc un rôle clef à jouer à la fois pour protéger le tissu économique mais aussi pour sensibiliser les entreprises, en particulier les TPE/PME, à leur exposition au risque cyber.

Le secteur de l'assurance est capable de se transformer pour prendre en charge ce nouveau risque et réaffirmer son rôle essentiel pour la résilience de notre économie. Dans l'histoire, l'assurance a su s'adapter aux transformations technologiques pour accompagner les entreprises et favoriser l'innovation. Les assureurs disposent de l'inventivité et des ressources pour appréhender ce risque et soutenir le tissu économique dans la transition numérique.

Il importe maintenant de travailler à la mise en œuvre des recommandations afin de permettre au marché de l'assurance du risque cyber d'atteindre sa pleine maturité et de faire de la place la Place de Paris un pôle d'expertise en matière d'assurance cyber. La poursuite des travaux engagés au sein d'une *task force* chargée de suivre et de coordonner les initiatives est ainsi essentielle. Les services de la direction générale du Trésor continueront d'être pleinement impliqués au service de la souveraineté et de la résilience de notre économie.

Synthèse

La numérisation de l'économie engendre de nouvelles vulnérabilités pour les entreprises. Si les technologies du numérique génèrent des gains de productivité et créent de nouveaux marchés, elles ont également conduit à l'émergence d'un nouveau risque : le risque cyber. Il renvoie à l'ensemble des risques liés à l'usage des technologies numériques et peut être défini comme un risque opérationnel portant sur la confidentialité, l'intégrité ou la disponibilité des données et des systèmes d'information. Il recouvre à la fois les actes malveillants mais aussi les incidents non intentionnels issus d'erreurs humaines ou d'accidents. La nouvelle dépendance du tissu économique au numérique ainsi que la rapidité de cette transition a facilité la multiplication de dommages ayant une origine cyber, en particulier les cyberattaques. La crise sanitaire a encore accéléré cette tendance, notamment à travers l'adoption de nouveaux modes de travail. Alors qu'elles s'accroissent en volume, fréquence et complexité, les cyberattaques sont aujourd'hui susceptibles de menacer la survie d'une entreprise. La résilience face au risque cyber constitue donc un enjeu majeur de souveraineté.

Or, l'assurance contre le risque cyber reste encore un marché peu développé. En 2021, le marché français du risque cyber est estimé à 219 millions d'euros de chiffres d'affaires, soit 3,1 % du total des cotisations de l'assurance des dommages aux biens des professionnels (7,07 milliards d'euros en 2021) et 0,35 % du chiffre d'affaires des assurances de biens et responsabilité[1].

Plusieurs freins au développement de ce nouveau produit ont été identifiés. Du côté de la demande, les entreprises, en particulier les TPE/PME, sous-estiment encore l'impact potentiel des attaques sur leur activité et ont du mal à identifier le contenu des offres proposées. Du côté de l'offre, les assureurs et les réassureurs ont des difficultés à mesurer ce risque protéiforme et évolutif, souvent en raison d'un manque de données. Ils craignent également de s'exposer à un risque qui peut parfois être de haute intensité et dont les caractéristiques rendent complexe la mutualisation (interconnexion des systèmes informatiques, hypothèse d'attaque aux dimensions systémiques, *etc.*). Enfin, les incertitudes entourant le cadre juridique de l'assurance du risque, notamment les couvertures implicites à travers des polices d'assurance traditionnelles ou encore la légalité des clauses remboursant le paiement des cyber-rançons, ne facilitent pas la structuration d'une offre.

Le marché de l'assurance du risque cyber, encore récent, peut constituer un levier de renforcement de la résilience des acteurs économiques. Ce marché connaît une croissance rapide : le volume des primes a ainsi augmenté de plus de 115 %[2] entre 2019 et 2021. Les entreprises prennent progressivement conscience des conséquences du risque cyber. Surtout, l'essentiel du risque cyber est maitrisable : 97 % des sinistres cybers couverts par une assurance ont donné lieu à une indemnisation inférieure à 3 millions d'euros 2021[3]. La priorité doit donc être de renforcer les capacités de mutualisation du marché de l'assurance cyber pour absorber les sinistres à haute intensité.

Dans ce contexte, il est recommandé de favoriser le développement du marché de l'assurance du risque cyber pour renforcer la résilience de notre économie et de faire de la Place de Paris un pôle européen d'expertise en la matière. À cette fin, la direction générale (DG) du Trésor a installé, le 30 juin 2021, un groupe de travail portant sur le développement d'une offre assurantielle de couverture des risques cyber. L'objectif de ce groupe de travail était de construire une offre d'assurance du risque cyber adaptée aux besoins de l'économie et aux enjeux de résilience et de

[1] Données France Assureurs.
[2] AMRAE, *LUmière sur la CYberassurance*, Juin 2022, mis en ligne le 9 juin 2022, consulté le 25 août 2022. URL : https://www.amrae.fr/bibliotheque-de-amrae?combine=&ref_id=4022&ref_type=publication&items=4022
[3] AMRAE, *LUmière sur la CYberassurance*, Juin 2022, mis en ligne le 9 juin 2022, consulté le 25 août 2022. URL : https://www.amrae.fr/bibliotheque-de-amrae?combine=&ref_id=4022&ref_type=publication&items=4022

souveraineté. Il a associé, outre les services de l'État, des représentants des entreprises, des entreprises d'assurance et de réassurance, des distributeurs d'assurance, des actuaires et des experts du monde académique et est animé par un comité de pilotage constitué de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), de l'Autorité de contrôle prudentiel et de résolution (ACPR), de l'Association pour le Management des Risques et des Assurances de l'Entreprise (AMRAE), de France Assureurs et de la DG Trésor.

A l'issue des travaux, le présent rapport propose un plan d'actions décliné en quatre axes :

(i) **Clarifier le cadre juridique de l'assurance du risque cyber.** La poursuite des efforts de clarification des clauses des contrats traditionnels constitue une priorité pour prévenir le phénomène des couvertures silencieuses. Le recours à des instruments de droit souple pour favoriser l'adoption des meilleures pratiques de rédaction est préconisé tout comme le renforcement de l'information des assurés sur l'étendue de leurs garanties. De plus, l'affirmation de l'assurabilité des cyber-rançons, conditionnée à un dépôt de plainte, ainsi que d'un principe général d'inassurabilité des sanctions administratives sont de nature à lever des ambiguïtés dommageables aux assurés comme aux assureurs.

(ii) **Favoriser une meilleure mesure du risque cyber.** Les meilleures pratiques remontées par les grands acteurs spécialisés notamment en matière d'évaluation de leurs risques à travers l'ORSA[4] pourraient être promues afin de mieux prendre en compte l'exposition des assureurs au risque opérationnel cyber. La création d'une catégorie ministérielle d'assurance et/ou d'une branche cyber dédiée permettrait d'améliorer le pilotage économique et réglementaire des passifs exposés au risque cyber. S'agissant de la problématique du manque de données, les bonnes méthodes de modélisation devront être utilisées en recourant, si nécessaire, à des méthodes innovantes. Le partage de données entre assureurs *via* une plateforme dédiée issue d'un partenariat public/privé est, enfin, recommandé.

(iii) **Améliorer le partage de risque entre assurés, assureurs et réassureurs.** Outre la promotion de solutions innovantes, comme l'assurance paramétrique, **le développement des captives de réassurance** peut offrir une réponse complémentaire à l'assurance du risque cyber. La mise en place d'une provision dédiée, en franchise d'impôt sur une période longue, est à cet égard une solution pertinente pour permettre aux entreprises de mieux gérer leur risque cyber en constituant des captives de réassurance.

(iv) **Accroître les efforts de sensibilisation des entreprises au risque cyber.** Il est ainsi préconisé de développer les coopérations entre acteurs publics et privés sur les territoires pour sensibiliser le tissu économique local ainsi que d'accroître les efforts de formation des professionnels de l'assurance. La définition de référentiels de sécurité partagés et un travail sur l'harmonisation des questionnaires de sécurité utilisés par les assureurs, constituerait également un levier pour améliorer la résilience cyber des entreprises et faciliter l'accès à l'assurance.

[4] *Own Risk and Solvency Assessment (ORSA).*

Synthèse des recommandations

Axe 1 : Clarifier le cadre juridique de l'assurance du risque cyber

Clarifier l'étendue des garanties cyber

Proposition 1 : Pour prévenir la survenance de couvertures cyber implicites, une communication de l'ACPR pourrait inviter les assureurs à i) rendre plus explicites les clauses de couverture et d'exclusion des risques cyber et ii) à mieux évaluer l'exposition de leur portefeuille d'assurance au risque.

Proposition 2 : Élaborer un guide de place rappelant le cadre juridique et les bonnes pratiques en matière de rédaction de contrats pour éviter les garanties implicites.

Proposition 3 : Renforcer l'information à destination de l'assuré pour mentionner explicitement la couverture ou l'absence de garantie du risque cyber dans les contrats professionnels.

Proposition 4 : Pour mieux évaluer et comprendre le phénomène, insuffisamment documenté, des couvertures non affirmatives, une étude de l'ACPR pourrait être conduite.

Clarifier les clauses litigieuses

Proposition 5 : Conditionner l'indemnisation d'une assurance cyber-rançons au dépôt de plainte de la victime afin de renforcer son accompagnement et améliorer les opérations d'investigation des autorités de police, justice et gendarmerie. En parallèle, une coopération accrue entre les assureurs et les forces de sécurité pourrait faciliter la lutte contre la cybercriminalité.

Proposition 6 : Affirmer un principe général d'inassurabilité des sanctions administratives dans le code des assurances.

Proposition 7 : Approfondir, en lien avec les parties prenantes, les travaux sur l'exclusion de garantie pour cause de cyberguerre.

Axe 2 : Mieux appréhender et mesurer le risque cyber

Améliorer la prise en compte du risque cyber dans l'activité assurantielle

Proposition 8 : Mieux prendre en compte l'exposition au risque opérationnel cyber des assureurs en l'incluant dans le rapport ORSA.

Proposition 9 : Pour améliorer le pilotage économique et réglementaire des passifs exposés au risque cyber, une catégorie ministérielle d'assurance cyber ainsi qu'une ligne d'activité spécifique pourront être créées. À moyen terme, une évolution de la réglementation européenne visant à créer une branche d'assurance dédiée permettrait de renforcer la qualité et la soutenabilité des couvertures cyber.

Répondre à la problématique du manque de données cyber

Proposition 10 : Mieux modéliser le risque cyber en s'appuyant sur les travaux méthodologiques des experts académiques. Des méthodes alternatives, telles que les approches bayésiennes ou le recours à l'intelligence artificielle, pourront apporter une première réponse pour appréhender ce risque en proie à un déficit de données.

Proposition 11 : Favoriser le partage des données de sinistralité cyber en créant un Observatoire de la menace cyber.

Axe 3 : Améliorer le partage du risque entre assurés, assureurs et réassureurs

Renforcer la résilience des entreprises

Proposition 12 : Développer le recours aux captives de réassurance notamment à travers la mise en place d'une provision dédiée facilitant la mutualisation des pertes sur un temps long. Étudier, à moyen terme, le développement des captives par compartiment.

Promouvoir des méthodes innovantes

Proposition 13 : Faciliter la constitution d'une offre d'assurance paramétrique pour permettre la couverture d'une partie du risque cyber.

Proposition 14 : Étudier le recours aux marchés financiers pour libérer de la capacité assurantielle.

Axe 4 : Accroitre les efforts de sensibilisation des entreprises au risque cyber

Encourager les PME à investir dans leur cybersécurité

Proposition 15 : Pour faciliter la souscription et mieux évaluer le niveau de maturité des entreprises, la mise en place de référentiels de sécurité adaptés selon leur profil ainsi qu'un travail sur une harmonisation des questionnaires de sécurité sont recommandés. Ces mesures permettront également aux entreprises d'identifier leurs expositions au risque cyber et à mettre en œuvre des mesures correctrices.

Proposition 16 : Mobiliser les réseaux de proximité, en s'appuyant sur les professionnels de la distribution de produits d'assurance, pour sensibiliser les TPE/PME au risque cyber.

Améliorer le capital humain

Proposition 17 : Améliorer la qualité de l'accompagnement des entreprises en développant la formation initiale et continue des professionnels du secteur de l'assurance.

Proposition 18 : Mettre en place une *task force* de l'assurance du risque cyber pour piloter le plan d'action de ce rapport et faire de la place de Paris un pôle d'expertise du risque cyber.

I. Malgré la multiplication des cyberattaques, le marché de l'assurance du risque cyber reste insuffisamment structuré pour se développer

1.1. Alors que le coût croissant des cyberattaques crée un besoin de couverture du risque par les assureurs, le marché de l'assurance du risque cyber peine à émerger

1.1.1 La numérisation de l'économie conduit à une multiplication des cyberattaques de plus en plus coûteuses

Le risque cyber est susceptible de revêtir des formes diverses pour les entreprises. Il renvoie à l'ensemble des risques liés à l'usage des technologies numériques et peut être défini comme un risque opérationnel portant sur la confidentialité, l'intégrité ou la disponibilité des données et systèmes d'information. Il peut s'agir d'une erreur humaine et non intentionnelle (transmission involontaire de données, téléchargement involontaire d'un logiciel malveillant notamment) ou même d'un accident. Il peut également s'agir d'une malveillance informatique volontaire (attaque d'un *hacker* via un logiciel installant un virus informatique, rançongiciel, attaque par déni de service). Les conséquences de la matérialisation du risque cyber peuvent être diverses pour une entreprise :

- des coûts de gestion immédiats de l'incident (frais de relations publiques pour gérer la crise, redirection vers un centre d'appel, recherche de cause, frais d'avocats, *etc.*) ;
- des frais liés aux conséquences financières directes subies par l'entreprise (frais de notification de violation de données personnelles, frais bancaires, frais nécessités par les enquêtes administratives, amendes administratives, *etc.*) ;
- des dommages directs subis tant immatériels (pertes d'exploitation, reconstitution des données, *etc.*) que matériels (destruction des biens physiques de l'entreprise) ;
- un engagement de sa responsabilité civile (indemnisation des dommages à un tiers, frais de défense, *etc.*) ;
- des coûts spécifiques liés à une cyber-extorsion (recours à un consultant, éventuel paiement de la cyber-rançon).

Cependant, la grande majorité des sinistres cyber est liée à une cyberattaque, dont le nombre connait une forte hausse depuis 2019. Selon l'AMRAE, les accidents ne sont la cause que de 5,5 % des sinistres en 2021 sur le marché de l'assurance du risque cyber[5]. L'augmentation des attaques affecte l'ensemble des acteurs économiques qu'ils soient des particuliers, des entreprises ou des institutions. La plateforme cybermalveillance.gouv.fr, chargée d'assister les victimes d'actes cyber malveillants, a enregistré une augmentation de sa fréquentation de 155 % entre 2019 et 2020 et de 101 % entre 2020 et 2021[6]. La même tendance est observée par le baromètre de la cybersécurité en entreprise CESIN 2022[7], qui estime que 54 % des entreprises françaises ont été attaquées en 2021. Les récentes attaques dirigées contre des établissements hospitaliers, tels que

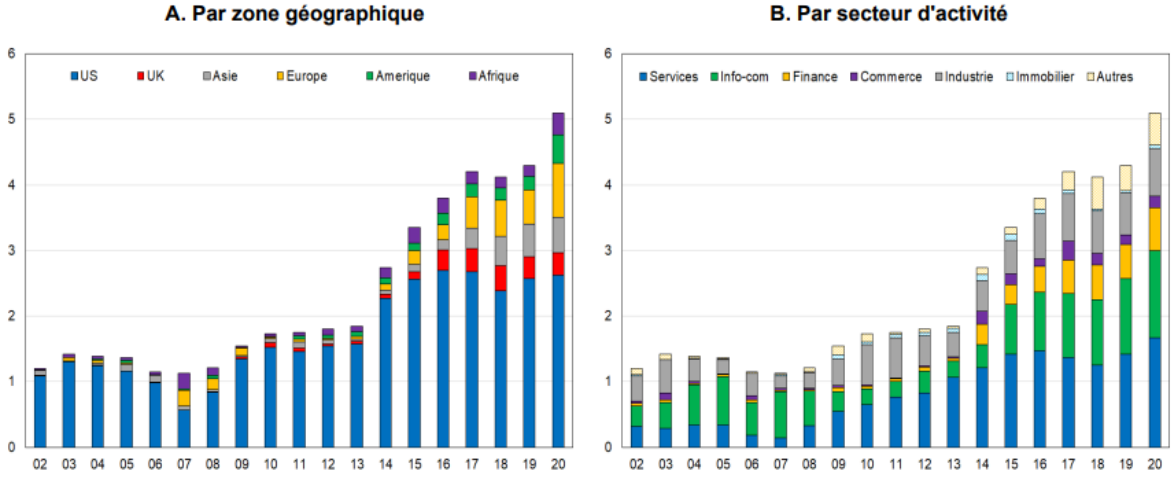
[5] AMRAE, *LUmière sur la CYberassurance*, Juin 2022, mis en ligne le 9 juin 2022, consulté le 25 août 2022. URL : https://www.amrae.fr/bibliotheque-de-amrae?combine=&ref_id=4022&ref_type=publication&items=4022

[6] Cybermalveillance, *Rapport d'activité 2021*, mis en ligne le 8 mars 2022, consulté le 11 mai 2022. URL : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/rapport-activite-2021

[7] CESIN, *Baromètre de la cybersécurité en entreprises,* mis en ligne le 17 janvier 2022, consulté le 11 mai 2022. URL : https://www.cesin.fr/actu-7eme-edition-du-barometre-annuel-du-cesin-enquete-exclusive-sur-la-cybersecurite-des-entreprises-francaises.html

ceux de Dax et de Villefranche-sur-Saône démontrent également que l'ensemble de l'écosystème, public ou privé, reste vulnérable. Dans sa cartographie prospective des risques 2022[8], France Assureurs place le risque cyber en tête du classement des risques pour la 5ème année consécutive.

Graphique 1 : Évolution du risque cyber



Note de lecture : Ces deux graphiques représentent la part des conférences de presse trimestrielles d'entreprises comportant une mention d'un ou plusieurs termes du champ lexical du risque cyber (en % du nombre total de conférences de presse comprises dans l'échantillon), agrégée par zone géographique et par secteur d'activité.
Source : Jamilov et al. (2021).

L'analyse de l'évolution du risque par zone géographique et par secteur met en évidence l'augmentation constante des attaques depuis 2007 (graphique A). Ces attaques se concentrent principalement sur les secteurs des services à la personne et de l'information et de la communication.

Bien qu'étant source d'opportunités et un vecteur majeur d'innovation, la transformation numérique s'accompagne donc de nouvelles vulnérabilités. La crise sanitaire a accéléré, à marche forcée, l'usage des outils dématérialisés qui ont été nécessaires à la continuité de l'activité économique et sociale en période de confinement ou de restriction de la mobilité physique. La généralisation du télétravail ou le suivi à distance de formations exposent davantage les utilisateurs aux attaques de cyber-délinquants. Le profil de ces attaquants n'est pas homogène : il peut s'agir d'acteurs qui évoluent au sein de l'organisation ciblée et qui ont des facilités d'accès au système informatique comme d'acteurs externes (États, groupes criminels ou hackers isolés). La commercialisation de logiciels malveillants sur internet a également créé un marché du « *crimeware as a service* » : l'accès au logiciel malveillant ainsi qu'à un ensemble de services *back-office* est proposé sous forme d'abonnement ou de partenariat. Ces acteurs redoublent d'inventivité pour mener à bien des actions d'extorsion, d'espionnage ou de déstabilisation.

Les outils et méthodes utilisés sont également en constante évolution : logiciels malveillants (*malwares* – installation sans consentement d'un logiciel indésirable, comme les rançongiciels), hameçonnage (*phishing* – tentative de récupération d'informations confidentielles en se faisant passer pour une entité connue), déni de service (*DoS* – attaque visant à rendre indisponible un service), attaques *man-in-the-middle* (interception de communications, sur un réseau wifi public par exemple), failles *zero-day* (exploitation d'une vulnérabilité jusqu'alors non-corrigée présente dans un logiciel).

Les coûts engendrés sont mécaniquement en progression même s'ils restent difficiles à estimer en raison du « chiffre noir » de la cybercriminalité qui désigne l'écart entre les actes connus et les actes réels et s'explique notamment par la crainte des victimes des conséquences néfastes sur

[8] France assureurs, *Cartographie prospective 2022 des risques de la profession de l'assurance et de la réassurance*, mis en ligne le 25 janvier 2022, consulté le 11 mai 2022. URL : https://www.franceassureurs.fr/nos-positions/lassurance-qui-protege/cartographie-prospective-risques-2022/

leur réputation. Ces coûts peuvent être directs, infligeant par exemple d'importantes pertes d'exploitation (coût d'un arrêt total de l'activité pendant plusieurs jours, coût de gestion de crise, éventuels frais de notification de pertes de données notamment) mais également indirectes avec des conséquences sur d'autres acteurs en raison des effets de contagion aggravés par les interdépendances numériques. Par exemple, la détection d'une faille informatique, en décembre 2021, au sein du module Log4j utilisé dans de nombreuses applications a créé une vulnérabilité pour tous les utilisateurs de ces applications. IBM Security, ayant mené une étude sur cette question du coût[9], a estimé qu'en moyenne une violation de données coûte 4,24 millions USD (plus 10 % entre 2020 et 2021). Cependant, la plupart des cyberattaques restent de faible intensité : en France, 92 % des sinistres n'ont représenté en 2021 que 7,4 % du total des indemnisations de l'assurance du risque cyber[10].

Le risque cyber devient ainsi de plus en plus présent dans la vie économique. Cependant, ce risque présente des caractéristiques particulières et doit être appréhendé différemment des autres grands risques. Tout d'abord, face à l'augmentation soutenue des attaques, les pertes pourraient s'alourdir considérablement dans le futur. Cela s'explique à la fois par l'augmentation progressive du coût des incidents cyber mais surtout par l'incertitude liée aux pertes potentielles futures résultant de méga-attaques ou de séries d'attaques de plus faible ampleur mais simultanées. Ces pertes sont également largement intangibles et difficiles à évaluer. Ensuite, les risques de cyberattaques sont potentiellement fortement corrélés en raison de l'interdépendance des systèmes informatiques et des acteurs économiques qui multiplie les probabilités de propagation des incidents. Également, et contrairement à d'autres grands risques, se pose la difficulté d'absence de données statistiques permettant de mieux comprendre et prévoir les attaques.

Pour agir sur la cybersécurité et assurer un niveau de sécurité suffisant des acteurs économiques, plusieurs réglementations ont été mises en œuvre : le projet de règlement sur la résilience opérationnelle numérique (règlement DORA) qui a pour objectif de permettre au secteur financier européen de maintenir des opérations résilientes en cas de perturbations cyber ou la directive *Network and Information System Security 2* (NIS 2) qui impose des normes de sécurité renforcées pour les entreprises européennes « essentielles ».

L'assurance, qui a pourtant un rôle clé à jouer dans la prise en charge de ce risque afin de permettre aux acteurs de mieux l'anticiper et y répondre, reste toutefois trop peu diffusée.

1.1.2 Pourtant, le marché de l'assurance du risque cyber demeure un marché de niche en France

L'assurance du risque cyber s'est développée à partir des années 1990 aux États-Unis. Au milieu des années 2000, le marché a connu une progression lors du développement de la réglementation sur les données personnelles aux États-Unis, imposant la notification aux victimes pour violation des données personnelles. Il a donc été nécessaire de proposer de nouvelles garanties permettant de prendre en charge ces frais qui peuvent être significatifs. Aujourd'hui, le marché mondial de l'assurance du risque cyber est estimé à environ 9 milliards USD[11], dont l'essentiel des primes est capté par le marché américain.

[9] IBM Security, *Cost of Data brech report 2021*.
[10] AMRAE, *LUmière sur la CYberassurance*, Juin 2022, mis en ligne le 9 juin 2022, consulté le 25 août 2022. URL : https://www.amrae.fr/bibliotheque-de-amrae?combine=&ref_id=4022&ref_type=publication&items=4022
[11] Munich Re, *Global Cyber Risk and Insurance Survey*, 2022

LE MARCHÉ DE L'ASSURANCE DU RISQUE CYBER AUX ÉTATS-UNIS

Le marché américain de l'assurance du risque cyber est un marché mature en forte croissance. En 2020, il représente 4,065 milliards USD de primes, soit une hausse de 29,1 % par rapport à 2019[12]**.** Il se caractérise par la part majoritaire des contrats cyber *stand alone* (2,579 milliards USD, soit 63,5 % du marché) par rapport aux contrats de police multirisques (1,485 milliard USD). Ces contrats dédiés connaissent une croissance continue (augmentation de +19 % par an en moyenne des primes entre 2016 et 2020 pour les assureurs domiciliés). Six acteurs domiciliés aux États-Unis représentent plus de 50 % du marché (Chubb, Axa XL, AIG, St Paul Travelers, Beazley, Axis capital).

Les États-Unis témoignent d'un niveau d'exposition relativement élevé et croissant aux cyberattaques. Entre l'année 2006 et la mi-2020, les États-Unis ont été le pays le plus touché par des cyber-attaques d'ampleur affichant des pertes supérieures à 1 million USD, avec 156 attaques[13]. Cette exposition reste dynamique : plus de la moitié des attaques recensées en 2020 et 2021 dans le monde visaient des acteurs américains[14]. Cette hausse de la sinistralité s'est traduite par un accroissement du niveau des primes et une dégradation de la rentabilité de l'assurance du risque cyber. Le *Government Accountability Office*[15] observe une forte augmentation des primes d'assurance sur les risques cyber en 2020 aux États-Unis, entraînant un surcoût de 10 à 30 % pour les assurés. Dans le même temps, entre 2019 et 2020, le ratio des sinistres rapportés aux primes pour les activités d'assurance du risque cyber aux États-Unis est passé de 45 à 67 %[16].

L'encadrement réglementaire et jurisprudentiel de l'assurance du risque cyber est croissant aux États-Unis. D'abord, la jurisprudence américaine relative à l'assurance des risques cyber, en cours de consolidation, contribue à préciser les contours de la responsabilité des assureurs. La jurisprudence tend à affirmer la spécificité du risque cyber et de sa couverture, notamment dans la définition des évènements couverts par les polices d'assurance contre les risques criminels[17] ainsi que dans le contenu et les exclusions des polices d'assurance spécifiques au risque cyber[18]. Par ailleurs, certaines autorités ont cherché à harmoniser les pratiques du secteur, notamment l'État de New York, qui a publié en février 2021 une directive visant à prescrire les bonnes pratiques pour le secteur[19].

Le marché de l'assurance du risque cyber demeure limité en France. Selon France Assureurs, le marché français du risque cyber est estimé à 219 millions d'euros de chiffres d'affaires en 2021, soit 3,1 % du total des cotisations de l'assurance des dommages aux biens des professionnels (7,07 milliards d'euros en 2021) et 0,35 % du chiffre d'affaires des assurances de biens et responsabilité. **Le marché reste essentiellement porté par les grandes entreprises**. Les entreprises qui réalisent

[12] NAIC 2021, *Report on the Cybersecurity Insurance Market.*
[13] SPECOPS, *The countries experiencing the most 'significant' cyber-attacks*, mis en ligne le 09 juillet 2020, consulté le 28 juin 2022. URL : https://specopssoft.com/blog/countries-experiencing-significant-cyber-attacks/
[14] COGNYTE, *Ransomware attack statistics 2021*, mis en ligne le 08 août 2021, consulté le 28 juin 2022. URL : https://www.cognyte.com/blog/ransomware_2021/ Ce chiffre ne retient toutefois que les cyberattaques recensées. Il est donc probablement en deçà du nombre effectif d'attaques, compte tenu du risque en termes d'image.
[15] GAO, *Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market*, mis en ligne le 20 mai 2021, consulté le 28 juin 2022. URL : https://www.gao.gov/products/gao-21-477.
[16] AON, *US Cyber Market Update - 2020 US Cyber Insurance Profits and Performance*, mis en ligne en juin 2021, consulté le 28 juin 2022. URL : http://thoughtleadership.aon.com/Documents/20210609-2021-cyber-market-update.pdf
[17] Voir notamment : *G&G Oil Co. of Indiana, Inc. v. Continental Western Insurance Co, 2021, Cour suprême de l'Indiana ;* Dans cette décision, la Cour juge que la police d'assurance contractée par la société G&G Oil, qui prévoit la couverture des pertes liées à la fraude informatique (*computer fraud*), inclut la couverture des pertes consenties dans le cadre du paiement de rançon consécutif à une attaque par rançongiciel.
[18] Voir notamment *Merck & Co., Inc. v. Ace American Insurance, 2022, Cour suprême du New Jersey.* La société Merck a subi en 2017 une attaque d'un groupe lié au gouvernement russe. Son assureur avance que cette attaque constitue un acte de guerre, de tels actes étant exclus des sinistres susceptibles d'être couverts par l'assurance. La Cour a débouté l'assureur et refuse la qualification d'acte de guerre.
[19] New york state, *Insurance Circular Letter No. 2*, mis en ligne le 04 février 2021, consulté le 18 juin 2022. URL : https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02

un chiffre d'affaires de 500 millions d'euros et plus ne totalisent que 5 % des contrats cyber autonomes (*stand alone*) souscrits mais représentent près de 75 % du chiffre d'affaires de l'assurance du risque cyber en 2021[20]. Cette situation explique que 80 % des cotisations de contrats cyber autonomes transite par les courtiers, 18 % par les agents et moins de 2 % pour les autres réseaux. **L'assurance du risque cyber reste peu répandue dans l'écosystème des PME et ETI** : ainsi, 84 %[21] des grandes entreprises sont couvertes par un contrat d'assurance du risque cyber pour seulement 9 % des ETI en 2021. Pour les PME, le taux de couverture est inférieur à 0,3 %. La sous-estimation du risque cyber par les plus petits acteurs ainsi qu'une maturité moindre aux enjeux de cybersécurité expliquent principalement cette tendance. Cependant, la souscription de contrats cyber dédiés se développe fortement chez les petites et moyennes entreprises.

Cependant, il s'agit d'un marché jeune en forte croissance. Avec une progression de 52 % des cotisations en 2021, l'assurance du risque cyber est le segment qui enregistre la plus forte croissance du marché des assurances de biens et responsabilité. La hausse du chiffre d'affaires en 2021 résulte à la fois d'une accélération de la demande de couverture mais également d'une revalorisation des primes pour faire face à la forte sinistralité enregistrée ces dernières années.

Les principaux assureurs du marché des risques d'entreprises proposent désormais tous une offre cyber. Les contrats cyber autonomes sont ainsi dédiés à la couverture des dommages résultant d'un fait générateur cyber. En 2021, près de 95 % des cotisations collectées pour le risque cyber émanent de contrats d'assurance dédiés[22]. **Les contrats classiques peuvent également contenir des garanties susceptibles de couvrir des dommages consécutifs à une cyberattaque**. Il peut s'agir de contrats de responsabilité civile (RC) qui pourront couvrir des dommages matériels aux tiers, des dommages immatériels consécutifs ou non, des dommages corporels aux tiers, des frais de justice ou encore la responsabilité civile des mandataires sociaux. Les garanties cyber peuvent également être présentes dans des contrats de dommages aux biens qui peuvent couvrir des dommages matériels touchant des biens physiques de l'entreprise (notamment marchandises, matériels, bâtiments), des pertes d'exploitation (pertes de marge brute, de recette, frais supplémentaires d'exploitation), des frais informatiques et des pénalités (pénalités de retard en particulier). A l'exception d'Axa, les principaux acteurs du marché de l'assurance du risque cyber en France sont soit américains, soit britanniques (Chubb, AIG, Beazley). **Les réassureurs jouent également un rôle dans la gestion du risque cyber**. Entre 35 % et 45 % des primes d'assurance du risque cyber seraient cédées aux réassureurs à l'échelle mondiale[23]. En France, plus de la moitié des membres de l'Association des professionnels de la réassurance en France (APREF) opèrent sur le marché de la réassurance du risque cyber.

[20] Données France Assureurs.
[21] AMRAE, *LUmière sur la CYberassurance*, Juin 2022, mis en ligne le 9 juin 2022, consulté le 25 août 2022. URL : https://www.amrae.fr/bibliotheque-de-amrae?combine=&ref_id=4022&ref_type=publication&items=4022
[22] Données France Assureurs.
[23] S&P Global Ratings, *Cyber risk in a new era: reinsurers could unlock the cyber insurance market*, 2021

1.2 Le marché de l'assurance du risque cyber peine à se développer en France, notamment en raison d'une insuffisante structuration du marché

1.2.1 Les incertitudes entourant le cadre juridique constituent un obstacle à la constitution d'un marché de l'assurance du risque cyber

a) La garantie implicite du risque cyber par des polices d'assurance traditionnelles est source d'incertitude sur la couverture de l'assuré, expose l'assureur à une perte non provisionnée et favorise le contentieux.

Le phénomène dit des « couvertures silencieuses » (*silent cover*) renvoie au fait qu'un contrat d'assurance dommages aux biens (DAB) ou encore d'assurance responsabilité civile peut couvrir des dommages consécutifs à la réalisation d'un risque cyber alors même que cette couverture n'est pas expressément mentionnée dans le contrat ni prise en compte dans sa tarification. Ainsi, un fait générateur cyber peut par exemple engendrer des conséquences matérielles dommageables (dommages physiques aux biens de l'assuré, perte d'exploitation) susceptibles d'être couvertes par un contrat dommages aux biens. De même, la divulgation de données à caractère personnel ou une cyberattaque interrompant les livraisons de l'entreprise peuvent d'engager la responsabilité civile de l'entreprise et donc d'être couvert par une police de responsabilité civile.

Les « couvertures silencieuses » en matière cyber sont source de difficultés tant pour l'assureur que pour l'assuré. Du côté de l'assureur, la police n'ayant pas été initialement rédigée à cette fin, le calcul de la prime ne prend pas en compte la réalisation de la conséquence du risque. Le portefeuille de l'assureur se trouve alors exposé à un risque cyber imprévu à travers cette garantie implicite. Cette situation n'est pas sans impact prudentiel : les provisions des assureurs pourraient être insuffisantes pour prendre en compte le risque cyber. Du côté de l'assuré, l'entreprise fait face à une incertitude sur l'étendue des dommages couverts, ce qui peut avoir un effet sur la demande en décourageant la souscription de police d'assurance du risque cyber. Certaines entreprises peuvent également se croire à tort couvertes contre l'intégralité des conséquences d'une cyberattaque et renoncer à souscrire à un contrat d'assurance du risque cyber dédiée. Cette situation engendre également une perte de temps : l'assuré peut ainsi être conduit à vérifier dans l'ensemble de ses contrats d'assurance s'il n'est pas implicitement couvert. Enfin, cette situation favorise également les refus de garantie opposés par l'assureur à l'assuré et donc des potentiels contentieux. Cependant, l'estimation de la part des contrats concernés est délicate dans la mesure où elle suppose d'analyser chaque contrat.

À la suite d'un communiqué de presse de l'ACPR[24] de novembre 2019 sur l'exposition des assureurs au risque cyber à travers les garanties implicites, les assureurs ont engagé un effort de clarification de leurs clauses. Après avoir cartographié leurs expositions au risque cyber, des assureurs ont progressivement introduit des garanties explicites ou des exclusions dans leurs polices traditionnelles. Par exemple, dans les contrats de dommages aux biens, les assureurs ont généralement exclu les « pertes d'exploitations sans dommage matériel » (PESD) à la suite d'un événement cyber. Ils ont également clarifié l'articulation entre les contrats cyber, responsabilité civile et dommages aux biens.

[24] ACPR, *Communiqué* : *La distribution des garanties contre les risques cyber par les assureurs*, mis en ligne le 12 novembre 2019, consulté le 28 juin 2022. URL : https://acpr.banque-france.fr/communique-de-presse/la-distribution-des-garanties-contre-les-risques-cyber-par-les-assureurs

Cependant, les pratiques hétérogènes d'exclusion du risque cyber sont susceptibles de renforcer l'incertitude sur l'étendue de la couverture de l'assuré, réduire la comparabilité de l'offre et générer du contentieux. Ainsi, la portée des exclusions n'est pas homogène entre assureurs. Cette situation peut avoir pour conséquence de renforcer l'incertitude sur la portée de la couverture assurantielle. Ainsi, dans de rares cas, en matière d'assurance de dommages aux biens, les dommages matériels et les pertes d'exploitation consécutives à un incendie dont l'origine serait cyber peuvent se retrouver exclus de la garantie. De plus, la définition des termes utilisés dans les polices (évènements cyber, système d'information de l'assuré, données) varie selon les assureurs et est parfois éloignée de celles utilisées par les professionnels des systèmes d'information. Ces divergences entre offres, limitant la comparabilité, constituent un obstacle supplémentaire à la souscription. Surtout, dans la mesure où les clauses d'exclusion sont soumises à un encadrement légal et jurisprudentiel strict, elles sont de nature à favoriser le contentieux et sont source d'insécurité juridique en cas de rédaction trop imprécise. La validité d'une clause d'exclusion relève en effet de l'appréciation souveraine des juges du fond.

Enfin, malgré les progrès réalisés, l'exposition actuelle des assureurs au risque cyber à travers des garanties implicites reste difficile à évaluer. La Fédération nationale des syndicats d'agents généraux d'assurance (Agéa) a mené une étude sur les contrats commercialisés en 2021 dans les réseaux d'agents généraux : sur onze contrats dommages aux biens trois n'excluaient pas clairement le risque cyber. Cependant, cette étude n'est pas représentative de l'ensemble du marché dans la mesure où les agents généraux s'adressent plutôt aux TPE/PME. Elle ne permet pas non plus de prendre en compte l'existence de couvertures silencieuses dans le stock d'anciens contrats.

b) Dans un contexte de fort développement des rançongiciels, l'assurabilité du paiement des cyber-rançons proposée dans de nombreux contrats est incertaine.

Un rançongiciel (*ransomware*) est un logiciel malveillant qui chiffre l'ensemble des données de la cible et lui demande une rançon en échange d'un mot de passe de déchiffrement. Cette pratique sanctionnée pénalement est de plus en plus utilisée par les cybercriminels[25].

[25] Les rançongiciels peuvent relever de plusieurs qualifications pénales : l'extorsion de fonds (article 312-1 du code pénal) ou l'infraction d'atteinte à un système de traitement automatisé de données (STAD) (article 323-1 du code pénal).

LE DÉVELOPPEMENT DES RANÇONGICIELS[26]

Les rançongiciels connaissent un fort développement dans la période récente. En France, en 2021 cybermalveillance.gouv.fr a reçu 1 851 demandes d'assistance pour des attaques informatique par rançongiciel, contre 996 en 2020 soit une hausse de plus de 85 %. Il s'agit d'un phénomène mondial : en 2020, 1 112 attaques réussies de rançongiciels étaient recensées dans le monde contre 1 097 sur le seul premier semestre 2021[27].

Bénéficiant de l'essor d'un écosystème criminel de plus en plus professionnel, les rançongiciels ont gagné à la fois en efficacité et en sophistication. Ainsi, la diffusion des crypto monnaies complexifie la traçabilité des opérations lorsque les rançons sont payées. De plus, certains groupes utilisent des informations privées dérobées comme moyen de pression supplémentaire mettant en œuvre une méthode de « double extorsion » : en plus de demander une rançon en échange du déverrouillage des données, les pirates menacent de rendre publiques des données privées. Enfin, depuis 2015, des rançongiciels se développent via un modèle économique spécifique : le *ransomware-as-a-service* (RaaS)[28] qui consiste à proposer l'accès sous forme d'abonnement ou de partenariat à un rançongiciel, ses infrastructures de paiement et de distribution ainsi qu'à un ensemble de services *back-office*, le tout sous une forme « prête à l'emploi ».

Si aucun secteur d'activité n'est épargné, l'ANSSI constate sur l'année 2020 **un ciblage notable des collectivités territoriales ainsi que des secteurs de l'éducation, de la santé et des services numériques**. Le secteur financier est également visé : dans le monde, 34 % des acteurs de l'industrie financière auraient fait l'objet d'une tentative d'attaque par rançongiciel[29]. L'ANSSI constate également une tendance au ciblage d'entreprise ou d'institution (*Big Game Hunting*), notamment à travers une préparation d'opération d'extorsion parfois plusieurs mois à l'avance[30].

Cette technique peut conduire à une perte élevée pour la victime pouvant mettre en péril la survie de l'entreprise. Selon les données enregistrées par la police et la gendarmerie, la valeur médiane de la rançon réclamée atteint 6 375 euros en 2020, en progression d'environ 50 % par an entre 2016 et 2020[31]. Le montant de la rançon peut parfois atteindre plusieurs millions d'euros. Les coûts directs liés au traitement de l'attaque, les coûts indirects liés aux pertes d'activité et les coûts liés aux indemnisations et aux amendes éventuelles viennent s'ajouter à l'éventuel paiement de la rançon.

Dans la mesure où le paiement ne garantit pas l'obtention d'un moyen de déchiffrement, incite les cybercriminels à poursuivre leurs activités, entretient ce système frauduleux et est susceptible de contribuer au financement du terrorisme[32], l'ANSSI recommande aux victimes de ne pas payer la rançon.

Des couvertures assurantielles contre les rançongiciels sont proposées par certains acteurs du marché. Ces contrats peuvent couvrir non seulement les dommages engendrés par l'attaque (les

[26] ANSSI, *Rapport 2021 : État de la menace rançongiciels à l'encontre des entreprises et institutions*, mis en ligne le 05 février 2021, consulté le 28 juin 2022. URL : https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-001/
[27] COGNYTE, *Ransomware attack statistics 2021*, mis en ligne le 08 août 2021, consulté le 28 juin 2022. URL : https://www.cognyte.com/blog/ransomware_2021/ Remarque : Ce chiffre ne retient que les cyberattaques recensées, probablement sous-estimées.
[28] Par exemple, les rançongiciels *Sodinokibi* (*alias REvil*), *DoppelPaymer*, *Maze*, *Netwalker*.
[29] SOPHOS, *The state of ransomware in financial services, septembre 2021.*
[30] Par exemple chaque échantillon des rançongiciels *RagnarLocker* et *DarkSide* est adapté à l'organisation ciblée.
[31] Attaques par rançongiciel envers les entreprises et les institutions. Études SSMI n° 37, 8 février 2022.
[32] Treasury's Office of Foreign Assets Control (OFAC*), Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*, publié le 21 septembre 2021. URL : https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf

frais de notification et frais de *monitoring* et surveillance, recours de tiers, pertes d'exploitations, *etc.*) mais aussi parfois le remboursement de la rançon payée. Selon une étude de France Assureurs, en 2022, sept compagnies d'assurance interrogées sur dix proposent cette garantie dans leurs contrats d'assurance cyber destinés aux TPE/PME[33]. Une telle garantie, qui prévoit le remboursement du paiement de la rançon, est susceptible d'encourager les cyberattaques par rançongiciel. Pour limiter ce risque, les assureurs mettent souvent en place des mesures de prévention afin d'essayer d'obtenir des informations sur les cybercriminels pour s'assurer du respect de leurs obligations de déclarations au titre de la lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB-FT) [34].

Le droit français ne prohibe pas explicitement l'assurabilité du paiement des cyber-rançons[35]. En permettant la solvabilité des victimes, le remboursement des cyber-rançons pourrait contrevenir à l'ordre public[36] en ce qu'il pourrait inciter à la commission d'infractions et serait susceptible de participer au financement d'organisations terroristes. Ce point n'a pas été tranché par la jurisprudence et le paiement d'une rançon tout comme son remboursement ne sont prohibés par aucun texte. D'une part, l'entreprise est victime d'une extorsion et agit donc sous la contrainte d'un groupe criminel. D'autre part, le remboursement d'une rançon par l'assureur est *a priori* licite et peut-être comparé à l'assurance couvrant le risque de vol dont le fait générateur est une infraction. Seule l'infraction de financement de terrorisme[37] est susceptible d'être invoquée mais ses conditions sont restrictives : l'entreprise payant la cyber-rançon ou l'assureur qui la rembourse doivent savoir que les fonds fournis sont destinés à être utilisés, en tout ou partie, en vue de commettre un acte de terrorisme. En matière cyber, l'identification de l'auteur et de la destination des fonds est rendue encore plus complexe. Aucun texte ou jurisprudence n'interdit explicitement à ce jour la couverture du risque de rançon.

c) La question de l'assurabilité des sanctions administratives se pose avec une acuité renouvelée dans un contexte d'accroissement du risque réglementaire pour les entreprises

Les obligations des responsables de traitement ainsi que les sanctions administratives infligées en cas de manquement ont été considérablement renforcées depuis le 25 mai 2018. Le règlement général sur la protection des données (RGPD) généralise en effet l'obligation de notification en matière de violation de données à caractère personnel[38]. En cas de manquement aux obligations du RGPD, la CNIL dispose d'un pouvoir de sanction renforcé qui peut atteindre 20 millions d'euros ou 4 % du chiffre d'affaires mondial[39] – la valeur la plus élevée étant retenue –, notamment en cas d'absence de notification par les responsables de traitement des violations de données personnelles. **Ce risque réglementaire amène les acteurs économiques à s'interroger sur la prise en charge par les assurances de ces sanctions administratives**.

Cependant, la couverture des conséquences des sanctions administratives contrevient au principe constitutionnel de personnalité des peines, bien qu'une telle règle ne soit pas expressément affirmée en droit positif[40]. Le principe constitutionnel de personnalité des peines, qui découle des articles VIII et IX de la Déclaration des Droits de l'Homme et du Citoyen de 1789

[33] Étude France Assureurs à partir d'un échantillon d'assureurs représentant 77% de part de marché de l'assurance du risque cyber.
[34] Les entreprises d'assurance sont notamment tenues de déclarer au service Tracfin « *les sommes inscrites dans leurs livres ou les opérations portant sur des sommes dont elles savent, soupçonnent ou ont de bonnes raisons de soupçonner qu'elles proviennent d'une infraction passible d'une peine privative de liberté supérieure à un an ou sont liées au financement du terrorisme* » (L. 561-15 du code monétaire et financier).
[35] Ce paragraphe reprend l'analyse du rapport du Haut comité juridique de la Place de Paris. Accessible via l'URL suivant : https://www.banque-france.fr/sites/default/files/rapport_45_f.pdf
[36] Les articles 6, 1102 et 1162 du code civil prohibent les conventions dont les dispositions contreviendraient à des règles d'ordre public.
[37] Article 421-2-2 du code pénal.
[38] Article 33 RGPD.
[39] Article 83 du RGPD et article 20 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[40] Ce paragraphe s'inspire de l'analyse du rapport du HCJP.

impliquant notamment que nul n'est punissable que de son propre fait, est applicable à toute sanction ayant le caractère d'une punition, qu'elle soit pénale, civile ou administrative[41]. Ce principe empêche qu'une autre personne que la personne sanctionnée puisse se substituer à elle dans l'exécution de sa peine afin de remplir son rôle punitif et dissuasif. L'assurabilité désinciterait, en effet, les responsables de traitement à se conformer à leurs obligations de protection de données personnelles. Ce principe fait obstacle à l'assurabilité des conséquences de telles sanctions. Deux arrêts de la Cour de cassation[42], où le bénéfice de la garantie d'une assurance des conséquences de sanctions a été écartée en raison de l'absence d'aléa (faute intentionnelle, connaissance du sinistre), ont pu être interprétés comme susceptibles de marquer une évolution dans le traitement de l'assurabilité de la sanction administrative. Cependant, la question de fond de la validité de l'assurance d'une sanction administrative n'est pas évoquée. Ils ne remettent donc pas en cause le caractère inassurable des sanctions administratives.

En pratique, de nombreux contrats d'assurance du risque cyber comportent des clauses couvrant les conséquences des sanctions administratives pécuniaires. Selon une étude de France Assureurs, en 2022, six compagnies d'assurance interrogées sur dix proposent une telle garantie dans leurs contrats d'assurance cyber proposés aux TPE/PME[43]. Ces clauses sont souvent rédigées en des termes généraux et comportent une réserve qui permet d'écarter le bénéfice de la garantie si elle est contraire aux limites fixées par la loi. Or, dans la mesure où ces clauses sont illégales, la garantie ne peut être utilement invoquée par l'assuré. Ces clauses sont susceptibles d'induire en erreur des entreprises, en particulier des TPE/PME, qui peuvent se croire couvertes, et de les désinciter à prendre les mesures nécessaires à leur cybersécurité.

d) L'absence de définition de la notion de cyberguerre engendre une incertitude sur une potentielle exclusion légale de garantie favorisant l'émergence de clauses d'exclusion conventionnelles hétérogènes

Pour les assurances de dommage aux biens, les risques de guerre sont légalement exclus de la garantie de l'assureur, sauf convention contraire. L'article L. 121-8 du code des assurances fixe un régime d'exclusion pour les « *dommages occasionnés soit par la guerre étrangère, soit par la guerre civile, soit par des émeutes ou par des mouvements populaires* ». La charge de la preuve repose sur l'assuré qui doit démontrer l'absence de lien de causalité entre le sinistre et un fait de guerre étrangère. Cette exclusion se justifie par le caractère inassurable d'une guerre qui constitue un risque de nature systémique générant des dommages massifs susceptibles de toucher tous les biens, limitant les possibilités de mutualisation.

L'applicabilité de la clause d'exclusion légale pour cause de guerre à un fait générateur de nature cyber est incertaine. Si la jurisprudence fait preuve de souplesse dans l'appréciation de cette exclusion pour cause de guerre étrangère[44], elle n'a cependant jamais défini la « guerre étrangère » au sens de l'article L. 121-8 du code des assurances. Cette exclusion légale, issue de la loi du 13 juillet 1930, n'a pas été pensée pour des cyberattaques dans un contexte international où le formalisme de la déclaration de guerre n'était pas encore tombé en désuétude. **En droit international, une cyberattaque par un autre État peut constituer un conflit armé international**. Les commentaires de 2020 aux Conventions de Genève de 1949 envisagent le cas où des cyberattaques peuvent donner lieu à un conflit armé international. Si ces attaques sont concomitantes d'opérations militaires classiques ou si elles entrainent des destructions équivalentes à de telles opérations, elles sont constitutives d'un conflit armé international.

[41] Cons. cons., 30 décembre 1987, n° 87-237 DC, Loi de finances pour 1988 ; CE, 28 juillet 1999, Syndicat des médecins libéraux et autres, n°s 202606 et s., aux T. ; CE, avis, 29 octobre 2007, Société sportive professionnelle LOSC Lille Métropole, n° 307736, p. 431

[42] Civ. 2ème, 14 juin 2012, pourvoi n° 11-17.367 ; Civ. 2ème, 13 juin 2019, n° 17-26.171.

[43] Étude France Assureurs à partir d'un échantillon d'assureurs représentant 77% de part de marché de l'assurance du risque cyber.

[44] La guerre englobe tous les faits qui se rattachent étroitement aux opérations de guerre sans qu'il soit besoin que le fait de guerre soit la cause unique ou directe du sinistre (Cass. civ. 24 et 25 juillet 1945, *Cie d'assurance Rhin et Moselle c. Lapel et Ane – Mutuelle de Rouen C. Bufacoux*).

Cependant, si les cyberattaques ont des effets plus limités sur les infrastructures civiles ou militaires, la qualification de conflit armé international n'est pas évidente et dépend de l'intensité de l'attaque. Enfin, l'acte doit être imputable à un autre État ou à un groupe sur lequel il exerce un contrôle effectif ou global.

Sans clause légale d'exclusion s'appliquant explicitement au risque de cyberguerre, des exclusions conventionnelles disparates pourraient émerger dans les polices d'assurance présentant le risque d'être interprétées de manière divergente et ainsi favoriser le contentieux. Aux États-Unis, à la suite de l'attaque *NotPetya*, certains assureurs anglo-saxons ont pu opposer des clauses d'exclusion conventionnelles donnant lieu à un contentieux émergent[45]. L'association du marché du Lloyd's (*Lloyd's Market Association*) a ainsi déjà publié en novembre 2021 quatre modèles de clauses d'exclusion de la cyberguerre permettant à l'assureur de démontrer l'origine étatique de l'attaque y compris en l'absence d'attribution officielle. Plutôt qu'une multitude de clauses conventionnelles rédigées de manière hétérogène, il apparaitrait préférable de disposer d'une clause unique d'exclusion pour des sinistres causés par un même risque.

1.2.2 Les difficultés à mesurer le risque cyber entravent la définition d'une offre cyber

La problématique de l'accès à la donnée, critère indispensable à une meilleure appréhension du risque cyber, constitue un défi majeur pour le développement du marché de l'assurance du risque cyber.

Dans le secteur de l'assurance, les données sont utilisées et analysées par la fonction actuarielle pour estimer la fréquence et l'ampleur des sinistres afin de tarifer au mieux le montant des primes. Traditionnellement, l'assureur utilise des données basées sur les pertes et sinistres passés ce qui permet d'estimer la probabilité de la survenance de futurs sinistres et leur gravité. Elles permettent ainsi d'évaluer le volume des provisions techniques nécessaires pour faire face aux sinistres.

Le risque cyber reste toutefois difficile à quantifier et ne peut s'analyser en utilisant seulement les méthodes traditionnelles usitées pour les autres grands risques. Ce risque, relativement récent, souffre d'un historique limité qui ne permet pas une modélisation statistique complète. Il s'agit également d'un risque évolutif et polymorphe qui émerge dans un contexte technologique en pleine expansion. Dès lors, l'observation des sinistres passés n'est pas forcément représentative et ne permet pas de prévoir efficacement les futurs sinistres.

Il existe également un grand flou autour des cyberattaques effectives. En effet, les organismes victimes communiquent peu sur les attaques subies et préfèrent en gérer les conséquences en interne. Elles craignent les effets négatifs sur leur réputation. Par conséquent, le nombre d'incidents déclarés reste très éloigné des attaques réelles. Le cadre réglementaire permet de se rendre compte de la réalité du phénomène : en effet, les exigences de *reporting*, telles que celles qui incombent aux entités critiques (opérateur d'importance vitale ou opérateur de services essentiels), permettent aux pouvoirs publics d'avoir accès aux incidents. Cependant, elles se limitent à une liste d'acteurs ciblés. Il en est de même pour les obligations de notification qui résultent d'une violation des données personnelles, prévues par l'article 33 du règlement général sur la protection des données (RGPD). Cette obligation ne concerne qu'un seul type d'incident cyber et ne permet pas d'avoir une vision de l'ensemble des incidents rattachés à une attaque. Hors exigences réglementaires ou législatives, les acteurs ne sont pas incités à faire remonter les attaques aux autorités ce qui ne permet pas une collecte de données et est préjudiciable à une meilleure appréhension du risque.

[45] Voir notamment Superior Court of New Jersey, 6 December 2021, *Merck & Co. Inc., and International Indemnity Ltd v. Ace American Insurance Company, et al.*

Enfin, il n'existe pas de base de données partagée liée aux incidents cyber, ni d'organisme ayant pour mission de collecter, de fiabiliser et d'anonymiser les incidents à l'échelle nationale. Les assureurs avancent ainsi avec une relative myopie ce qui constitue un risque en matière de soutenabilité du marché de l'assurance du risque cyber et peut également engendrer une tarification inadaptée dommageable autant à l'assureur qu'à l'assuré.

1.2.3 Dans un contexte de contraction des capacités assurantielles et réassurantielles, les caractéristiques du risque cyber limitent les possibilités de couverture

a) Le coût potentiellement élevé et les spécificités du risque cyber pèsent structurellement sur les capacités des assureurs et réassureurs à le couvrir

Le coût d'une cyberattaque de haute intensité peut être élevé, ce qui oblige les assureurs et réassureurs à y consacrer des capacités importantes au détriment d'autres risques. Pour couvrir un risque, l'assureur est conduit à provisionner des fonds pour indemniser l'assuré en cas de sinistre. Or, si le coût du sinistre est très élevé, la capacité de l'assureur à prendre en charge ce risque est plus limitée. Les sinistres de haute intensité peuvent engendrer une indemnisation significative de l'assureur : selon l'AMRAE[46] la hausse du montant (multiplication par trois, de 73 millions d'euros en 2019 à 217 millions d'euros en 2020) des indemnisations en France entre 2019 et 2020 n'est due qu'à quatre sinistres de très haute intensité (entre 10 et 40 millions d'euros d'indemnisation chacun), soit 1 % des sinistres indemnisés en 2020. Selon le rapport Hiscox d'avril 2021 sur la gestion des cyber-risques[47], 5 % des cyberattaques sur les entreprises de plus de 1 000 salariés engendrent des dommages supérieurs à 420 000 euros, soit un niveau presque 40 fois supérieur au coût médian. Cette situation est accentuée par le fait qu'il existe une forte incertitude sur les pertes potentielles des cyberattaques dans un contexte d'accroissement tendanciel de leur coût, renforcé par le sous-investissement des entreprises dans leur cybersécurité et l'approfondissement du cadre réglementaire. **Dans certains cas, le risque cyber pourrait même prendre les caractéristiques d'un risque systémique**. Une étude de la Fed de New York[48] modélise les conséquences d'une éventuelle cyberattaque d'ampleur sur un acteur majeur du système bancaire et conclut à leur similarité avec celles d'un épisode de panique bancaire (*bank run*). Ses auteurs estiment qu'une telle attaque serait susceptible de générer un choc sur la liquidité et entraîner un coût financier pouvant atteindre 122 milliards USD le premier jour et jusqu'à 1 000 milliards USD au cinquième jour.

Les possibilités de diversification du risque cyber sont réduites sous l'effet de l'interconnexion des systèmes d'information. Internet conduit à relier les systèmes d'information entre eux, ce qui favorise les contagions en cas de cyberattaque. Ce risque est encore accru par la concentration des plateformes et systèmes d'exploitation en raison des effets de réseau et des économies d'échelle qui caractérisent l'économie du numérique[49]. Ainsi, une faille informatique sur un système d'exploitation rend vulnérables toutes les entreprises qui l'utilisent. De même, la diversification géographique est entravée dans la mesure où une cyberattaque peut affecter tout un pays voire le monde entier. Ainsi, en mai 2017, le rançongiciel *WannaCry* a infecté en une

[46] AMRAE, *LUmière sur la CYberassurance*, Juin 2022, mis en ligne le 9 juin 2022, consulté le 25 août 2022. URL : https://www.amrae.fr/bibliotheque-de-amrae?combine=&ref_id=4022&ref_type=publication&items=4022

[47] HISCOX, *Rapport 2021 sur la gestion des risques cyber « Cyber-résilience: Ne jouez pas l'avenir de votre entreprise aux dés ! »,* mis en ligne en avril 2021 et consulté le 28 juin 2021. URL : https://www.hiscox.fr/courtage/sites/courtage/files/documents/21486%20-%20Hiscox%20Cyber%20Readiness%20Report%202021%20-%20France.pdf

[48] Thomas EISENBACH, Anna KOVNER, et Michael JUNHO LEE, "Cyber risk and the U.S. financial system: A pre-mortem analysis," *Journal of Financial Economics*, 2021. DOI : https://doi.org/10.1016/j.jfineco.2021.10.007

[49] Voir sur les plateformes Trésor-Éco n° 250, *Plateformes numériques et concurrence*, 2019, Marion Panfili. URL : https://www.tresor.economie.gouv.fr/Articles/7690058a-00e4-44a7-8aed-9a2ee5a04d51/files/c888861f-5516-4e4e-b3ce-a96af66b3c34

journée au moins 200 000 machines dans plus de 150 pays en exploitant une faille de sécurité dans le système Windows, se diffusant automatiquement et très rapidement.

Ce constat ne signifie pas pour autant que le risque cyber est inassurable dans la mesure où les conséquences de la plupart des sinistres de nature cyber restent maitrisables. En 2021, 97 % des sinistres cybers couverts par une assurance ont donné lieu à une indemnisation inférieure à 3 millions d'euros[50]. De même, les conséquences de sinistres cyber de haute intensité restent inférieurs à ceux d'autres risques comme les catastrophes naturelles. Ainsi, les dommages de la tempête Alex sont estimés à 220 millions d'euros et 1 milliard d'euros pour les dommages sur des infrastructures publiques. **La réflexion sur une éventuelle intervention publique pour prendre en charge le risque cyber apparaît prématurée, la priorité étant de mieux appréhender le risque et de développer le marché de l'assurance cyber afin de renforcer les capacités de mutualisation des acteurs.** La mutualisation permettra en effet de limiter la volatilité et d'absorber les sinistres de plus forte intensité, ce qui suppose d'améliorer le taux de couverture. Le développement des captives de réassurance ou encore les mesures concernant les opérateurs d'importance vitale potentiellement systémique sont également de nature à prévenir ce risque.

b) La contraction des capacités assurantielles et réassurantielles et la dégradation de la sinistralité cyber accélèrent la tendance au durcissement des conditions d'assurance du risque cyber, en particulier pour les grandes entreprises

Le marché des risques d'entreprise est un marché cyclique. Depuis le début des années 1990, il connaît des phases successives de hausse puis de baisse du niveau des primes. Le dernier cycle baissier a commencé en 2004-2005 et a duré près de 15 ans. Il s'est achevé en 2019 aux États-Unis puis en Europe conduisant à un durcissement des conditions de souscription. Cette tendance touche en premier lieu les garanties dommages aux biens souscrites par des entreprises – même si d'autres risques tels que les responsabilités civiles générale, professionnelle ou environnementale sont concernés. Cette sélectivité affecte principalement les grands risques, dont le risque cyber. Cette situation s'explique par la hausse de la sinistralité liée à la pandémie de la COVID-19 mais aussi aux catastrophes naturelles, notamment aux États-Unis avec l'ouragan Laura et les vents violents du *Midwest Derecho*. Enfin, il existe un effet de correction à la hausse des tarifs consécutif à quinze années de baisse tarifaire.

En France, la dégradation de la sinistralité en 2020 en matière cyber a entraîné un durcissement marqué des conditions d'assurance pour les grandes entreprises. Selon l'étude LUCY de l'AMRAE, la sinistralité a été multipliée par trois entre 2019 et 2020, passant de 73 millions d'euros à 217 millions d'euros avant de diminuer en 2021 à 164 millions d'euros[51]. Le ratio combiné (sinistres/primes) connait un mouvement similaire : il est ainsi passé de 84 % en 2019 à 167 % en 2020 avant de redescendre à 88 % en 2021. Ces résultats techniques varient fortement en fonction de la taille de l'entreprise : en 2020, le ratio sinistres/primes de 190 % pour les grandes entreprises expliquait à lui seul les pertes de l'assurance du risque cyber. En conséquence, l'AMRAE[52] constate un quasi-doublement des tarifs pour les grandes entreprises entre 2020 et 2021 : le taux de prime[53] a augmenté de 97 %. Les ETI ont également connu une forte hausse de plus de 56 % sur la même période[54]. Le niveau des franchises a également augmenté à près de 4 millions d'euros en moyenne pour les grandes entreprises. La prise de conscience de la réalité des expositions et la complexification du risque dans un contexte inflationniste devraient conduire à faire progresser encore davantage le niveau des primes. L'aggravation de la sinistralité constatée pour le segment des ETI (ratio sinistre/primes de 261 % en 2021 selon l'AMRAE) devrait également alimenter cette hausse. **Cette situation se traduit par des difficultés accrues pour les grandes**

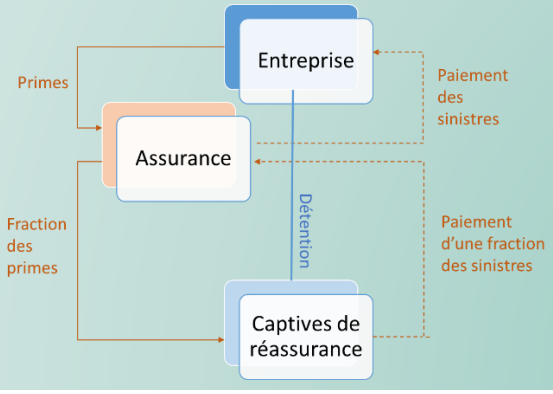
[50] AMRAE, *LUmière sur la CYberassurance*, Juin 2022, mis en ligne le 9 juin 2022, consulté le 25 août 2022. URL : https://www.amrae.fr/bibliotheque-de-amrae?combine=&ref_id=4022&ref_type=publication&items=4022
[51] *Ibid.*
[52] *Ibid.*
[53] Rapport entre les primes pratiquées et la capacité moyenne souscrite.
[54] Les ETI continuent de payer leur couverture deux fois moins cher que les grandes entreprises.

entreprises pour s'assurer. Les grandes entreprises, dont le risque cyber est plus complexe à évaluer, sont insuffisamment couvertes au regard de leurs expositions. En 2021, elles souscrivent en moyenne une couverture de 31 millions d'euros alors que les attaques visant les grandes entreprises peuvent entraîner des pertes s'élevant à plusieurs centaines de millions d'euros (250 millions d'euros sur les ventes du groupe Saint-Gobain en 2017). Les assureurs prêts à prendre le rôle d'apériteur[55] du programme d'assurance du risque cyber d'un grand compte sont de plus en plus rares. Le taux de couverture des grandes entreprises a ainsi diminué de 4,4 points entre 2020 et 2021 selon l'AMRAE, ce qui limite encore davantage les capacités de mutualisation de l'assurance du risque cyber.

c) Les entreprises disposent de peu de solutions d'auto-assurance pour pallier la contraction des capacités assurantielles

La constitution de captives de réassurance, outils d'auto-assurance complémentaire à l'assurance et à la réassurance privée, pourrait contribuer à protéger l'activité des entreprises face aux risques cyber. Les captives de réassurance sont des organismes de réassurance qui limitent leur activité à la souscription des risques de leur groupe et qui ont été placés dans un premier temps chez un assureur tiers. D'une part, elles permettent une meilleure gouvernance et une meilleure maîtrise des risques : la mise en place d'une captive de réassurance professionnalise la gestion interne du risque (identification, mesure, maîtrise et prévention). D'autre part, elles offrent une opportunité de mutualisation financière à travers le cycle économique : les provisions qu'elles constituent permettent un lissage dans le temps en absorbant les chocs exogènes, ce qui les rend particulièrement adaptées à la gestion des risques exceptionnels. La constitution de captives est ouverte à toutes les entreprises. L'intervention d'un assureur tiers permet à l'entreprise de bénéficier de l'accompagnement dans l'évaluation des risques ainsi que dans les niveaux de rétention et constitue un facteur de bonne gestion de la captive.

FONCTIONNEMENT D'UNE CAPTIVE DE RÉASSURANCE



La captive de réassurance présente plusieurs avantages en comparaison des captives d'assurance. En premier lieu, grâce à l'implication d'assureurs en première ligne, les entreprises industrielles sont mieux accompagnées tant dans la définition et l'évaluation des risques que dans les niveaux de rétention. De plus, la captive de réassurance est tenue à une bonne gestion (provisionnement adéquat, gouvernance de qualité) du fait de sa relation commerciale avec un assureur (nécessité d'un alignement d'intérêt). Par ailleurs, la captive de réassurance ayant un accès aux informations concernant les risques réassurés, offre des possibilités de montages plus fins et plus adaptés au profil de risque du groupe auquel elle appartient. Elle contribue ainsi à la meilleure maîtrise des

[55] Assureur principal, qui établit et gère le contrat dans le cas d'une coassurance. Lorsque les risques à couvrir sont jugés trop importants pour être supportés par une seule entreprise d'assurances, la société pressentie par l'assuré, convient avec d'autres sociétés d'assurances de partager les profits et les risques mais, sans solidarité entre elles. L'assureur qui prend la tête du groupe, est généralement celui qui a négocié le contrat avec l'assuré.

risques par des groupes non financiers et à la prévention des sinistres. Enfin, dans un environnement assurantiel tendu en termes de capacités offertes et de prix, la captive de réassurance permet un accès à des capacités supplémentaires via des rétrocessions à des réassureurs, avec lesquels les entreprises ne pourraient pas traiter directement.

Cependant, l'écosystème français apparaît insuffisamment favorable à l'émergence de captives de réassurance. Ainsi, la France compte actuellement sept captives de réassurance contre 234 au Luxembourg, 831 aux Bermudes et 49 en Suède. Le Luxembourg offre des solutions clef en main auxquelles les entreprises continueront de recourir. Cet état de fait empêche le développement d'un écosystème (actuariat, conseil financier et audit, courtage) qui émergerait pour accompagner les entreprises dans leurs démarches. De plus, l'accès à des captives dans des juridictions étrangères demande des ressources dont les plus petites entreprises ne disposent pas, les privant de cet outil d'auto-assurance. **L'absence de provisions adaptées aux captives de réassurance et ouvertes au risque cyber constitue un frein à leur développement**. Actuellement, il n'est possible de recourir qu'aux provisions pour égalisation[56]. Utilisées en réassurance et en assurance de branches cycliques (catastrophes naturelles, assurance-crédit), ces provisions bénéficient d'un régime fiscal favorable : leur dotation est déductible temporairement de l'assiette de l'impôt sur les sociétés[57]. Cependant, le champ des provisions d'égalisation reste strictement limité à certains risques précisément identifiés et ne couvre pas le risque cyber. De plus, les paramètres techniques des provisions pour égalisation (périmètre des risques couverts, modalités de constitution et de déductibilité) ne sont pas adaptés aux risques portés par une captive de réassurance, qui concernent uniquement les sociétés de son propre groupe. Ces paramètres correspondent davantage aux caractéristiques d'assureurs ou de réassureurs qui sont en mesure de mutualiser les risques entre plusieurs clients : les provisions pour égalisation ne sont pas fongibles entre les différents types de risque couverts et leur horizon temporel est fixé entre 10 et 15 ans selon la nature du risque.

1.2.4 La sous-estimation du risque cyber et l'accompagnement encore insuffisant des entreprises réduisent la demande d'assurance du risque cyber

Au niveau de la demande, le développement du marché de l'assurance du risque cyber se heurte à une sous-estimation des acteurs face au risque.

Les acteurs sous-estimant ce risque peuvent avoir tendance à sous-investir en matière de cybersécurité. En effet, malgré une augmentation continue des attaques, le degré de cybersécurité des entreprises françaises demeure insuffisant. Le dernier rapport d'Hiscox[58] sur la gestion des risques cyber révèle que près de la moitié d'entre elles ont subi au moins une attaque en 2020.

Même s'il concerne l'ensemble des entreprises, le risque cyber est mieux pris en compte par les grandes entreprises dont le niveau de maturité cyber est en constante augmentation. C'est, en effet, ce que constate Wavestone dans son rapport publié en 2022[59]. Il apparait que le niveau de maturité général des entreprises françaises est au-dessous de la moyenne (46 %) avec d'importantes disparités entre secteurs d'activité. À titre d'exemple, le secteur financier présente une maturité de 54,4 % alors que les services et le secteur public ont, respectivement, un niveau de maturité de 42,5 % et 36,9 %. Les entreprises assujetties à des réglementations en matière de

[56] Définies à l'alinéa 6° de l'article R. 343-7 du code des assurances pour les opérations d'assurance non-vie.
[57] Dans des plafonds et selon des modalités précisées par les articles 39 quinquies G et suivants du code général des impôts.
[58] Hiscox, *Cyber Readiness Report 2021 – France*, mis en ligne en avril 2021, consulté le 15 mai 2022 URL : https://www.hiscox.fr/courtage/sites/courtage/files/documents/21486%20%20Hiscox%20Cyber%20Readiness%20Report%202021%20-%20France.pdf
[59] Wavestone, *Cybersécurité : où en sont les entreprises françaises ?,* mis en ligne le 16 mars 2022, consulté le 20 mai 2022 URL : https://www.wavestone.com/fr/communiques-de-presse/cybersecurite-ou-en-sont-les-grandes-organisations-francaises/

sécurité des infrastructures (Loi de programmation militaire ou directive européenne NIS, *Network and Information Security*) sont également plus matures que la moyenne.

Pour faire face à l'augmentation des attaques, les entreprises se sont dotées d'un arsenal d'outils et de services informatiques. Cela constitue un investissement qui peut être conséquent surtout pour les petites et moyennes entreprises. L'étude Hiscox, indique que failles utilisées par les attaquants proviennent autant d'erreurs humaines (28 %) que de vulnérabilités provenant des outils informatiques (37 % des attaques utilisent les serveurs de l'entreprise). Il existe également une perception face au risque différente entre les équipes informatiques et les équipes « métier » en raison de la technicité du sujet. Les dirigeants d'entreprises ont souvent du mal à percevoir le retour sur investissement et se reposent sur les experts internes ou externalisent la protection du système informatique. Au surplus, il s'agit d'un risque face auquel les acteurs ne sont pas égaux en raison d'importantes asymétries d'information face au numérique et d'un plus faible taux de survie des petites et moyennes entreprises après une cyberattaque.

La sous-perception du risque est très marquée pour les TPE/PME. Lors de son étude LUCY, l'AMRAE a ainsi observé que seulement 322 PME sur 140 000 réalisant entre 10 et 15 millions d'euros de chiffre d'affaires ont souscrit une assurance du risque cyber en 2021. Cette sous-perception peut s'expliquer par différents facteurs. Tout d'abord, ces entreprises ont un budget restreint et l'investissement dans une assurance facultative cyber supplémentaire ne semble pas prioritaire. De plus, la culture de gestion de l'activité et de gestion des risques est peu développée. Enfin, elles craignent moins les conséquences négatives en matière d'image lors d'une attaque car elles sont peu exposées médiatiquement.

La complexité et l'hétérogénéité des questionnaires utilisés par les assureurs peuvent freiner la demande d'assurance du risque cyber chez les PME/TPE sans renseigner de manière satisfaisante sur l'exposition au risque de l'entreprise. Ces questionnaires, visant à établir le niveau de sécurité d'une organisation souhaitant souscrire une police cyber, constituent une charge administrative significative pour l'entreprise : chaque assureur dispose de son propre questionnaire qui peut varier pour une même entreprise en fonction des sujets traités ou de la zone géographique. Surtout, ils ne permettent pas de renseigner efficacement sur le niveau de risque de l'entreprise. Ils sont souvent peu adaptés à la taille et aux spécificités de l'entreprise. Les questions posées ne permettent pas d'apprécier l'efficacité des dispositifs de cybersécurité opérationnels mis en œuvre. De plus, la défense en profondeur ne peut être prise en compte dans ces tests réalisés depuis l'extérieur des organisations qu'elles tentent de cibler. Les questionnaires sont peu sécurisés : un groupe d'attaquants qui arriverait à s'infiltrer dans le réseau de l'un de ces acteurs, pourrait récupérer ces questionnaires et connaîtrait ainsi précisément la cartographie des moyens de défense d'un certain nombre d'entreprises avec leurs points forts mais aussi leurs vulnérabilités

Toutefois, en l'absence d'une sécurisation des systèmes informatiques et d'une couverture assurantielle, ces attaques peuvent compromettre la survie des entreprises. Le rapport d'Hiscox indique que, si le coût médian d'une cyberattaque reste maitrisable (9 000 euros pour les entreprises de 50 à 249 salariés et 15 000 euros pour les entreprises de 250 à 999 salariés), 5 % des entreprises de 50 à 249 salariés subissent des dommages de l'ordre de 108 000 euros (respectivement 347 000 € pour les entreprises de 250 à 999 salariés). Une étude de 2020 du cabinet Bessé[60], note également que lorsqu'une entreprise subit une cyberattaque, elle double son risque de défaillance.

À cette sous-perception du risque, s'ajoute également des difficultés de distribution des offres de la part des intermédiaires[61]. L'Agéa a effectué en 2020 une étude interne sur son réseau pour

[60] GROUPE BESSE, *Crise cyber : quel impact sur la valorisation des entreprises non cotées ?*, mis en ligne en novembre 2020, consulté le 10 juin 2022. URL : https://www.besse.fr/sites/default/files/2020-12/ETUDE%20CYBER%20BESSE%202020%20PLANCHE.pdf

recueillir la perception des agents généraux face au risque cyber. Ces derniers ont indiqué manquer de connaissance du risque cyber qui reste très technique. Ils préfèrent ainsi commercialiser des garanties qu'ils maitrisent davantage. Ils ajoutent également que le processus de souscription peut être lourd et onéreux pour les clients. Ils pointent également du doigt l'absence ou la faible culture du risque des TPE/PME. L'ensemble de ces éléments rend difficile l'identification de leviers de souscription.

Pour favoriser la perception du risque de la part des entreprises et accroitre leur maturité, il semble ainsi autant nécessaire d'agir sur la sensibilisation des acteurs que sur la culture du risque.

II. Le développement de l'assurance du risque cyber passe par une clarification de son cadre juridique, l'adoption d'outils et de pratiques visant à mieux le mesurer et le partager ainsi que par des efforts accrus de sensibilisation et d'accompagnement des entreprises

2.1. La clarification du cadre juridique faciliterait la constitution d'un marché de l'assurance du risque cyber

2.1.1 L'adoption de bonnes pratiques de rédaction des contrats voire une obligation renforcée d'information permettraient de clarifier l'étendue des garanties cyber

Alors que le phénomène des couvertures silencieuses génère une incertitude sur le champ de la garantie, préjudiciable tant à l'assureur qu'à l'assuré, **l'effort de clarification des clauses des polices d'assurance est à poursuivre pour permettre au marché de l'assurance du risque cyber de se développer**. À ce titre, les clauses dites « affirmatives », listant explicitement les faits générateurs couverts par la police d'assurance, limitent les garanties implicites du risque cyber. Cette démarche devra s'opérer en préservant la couverture des assurés.

BONNES PRATIQUES DE RÉDACTION DE POLICES D'ASSURANCE

Les polices d'assurance peuvent prendre deux formes :

- Le contrat peut être dit **« tous risques sauf… »** : l'ensemble des risques est couvert sauf les risques explicitement cités dans le contrat. Ces formules peuvent contenir des couvertures silencieuses. L'enjeu devient de rédiger clairement la clause d'exclusion ;
- Les contrats dits **« périls dénommés »** couvrent uniquement les évènements expressément dénommés. Ce type de contrat permet d'éviter des garanties implicites. Les polices de tradition *Common Law* sont majoritairement construites sous la forme dite des « périls dénommés ».

Les définitions de notions clefs, comme « dommages matériels » ou « dommages immatériels », sont souvent rédigées sans prendre en compte le risque cyber. Ainsi, lorsque le dommage matériel recouvre « *la détérioration la disparition, l'atteinte, l'altération, la destruction, la disparition, la perte, le vol* » d'une « *chose, d'une substance ou d'une valeur* », les biens incorporels informatiques (données, systèmes d'information) peuvent être qualifiés de dommages matériels au sens du contrat. Pour limiter ce risque, il est préférable de recourir à des termes moins ambigus comme « biens corporels » à la place de « chose ». Il est également souhaitable de coordonner entre elles les définitions – matériel et immatériel – pour s'assurer que le risque cyber relève clairement de l'une ou de l'autre catégorie. De même, les termes désignant les biens assurés

gagneraient à être choisis en tenant compte du risque cyber. Par exemple, la notion de « supports informatiques » est très englobante (disque durs, logiciels). Le glossaire de l'ANSSI[62] pourra également constituer une ressource utile pour la définition de termes techniques lorsque sa mise à jour sera intervenue.

Une vigilance particulière est à porter aux clauses d'exclusion, qui doivent rester « formelles et limitées » (article L. 113-1 du code des assurances) et être mentionnées en caractères très apparents (article L. 112-4 du code des assurances). Ainsi, une exclusion trop large peut être jugée invalide. La validité de la clause relève de l'appréciation souveraine des juges du fond. La jurisprudence est stricte : la Cour de cassation considère que la seule présence d'un cas imprécis entache d'illégalité l'ensemble des cas énumérés dans la clause d'exclusion[63]. Il est important d'éviter les termes imprécis comme « et autres », « tels que » ou encore « par exemple ».

À court terme, la diffusion des meilleures pratiques en matière de rédaction de clauses permettrait de clarifier les garanties des contrats.

Une communication de l'Autorité de contrôle prudentiel et de résolution (ACPR) pourrait inviter les assureurs à rendre plus explicites les clauses de couverture et d'exclusion des risques cyber et à leur rappeler la nécessité d'évaluer de façon exhaustive l'exposition de leur portefeuille d'assurance au risque cyber. Une telle approche s'inscrirait dans la continuité du communiqué de presse du 12 novembre 2019 de l'ACPR sur « *la distribution des garanties contre les risques cyber par les assureurs* ». Elle pourrait être complétée par la mise à jour du glossaire de l'ANSSI sur la terminologie cyber.

Cette communication [64] enverrait un signal fort à l'ensemble des acteurs de la place. Bien que n'étant pas d'ordre réglementaire, cette communication pourrait contribuer à uniformiser les pratiques des assureurs, permettant l'adoption des meilleures pratiques, notamment des grands acteurs spécialisés. Elle ne pourra cependant pas définir juridiquement l'évènement cyber, ni imposer des clauses d'exclusion ou les risques couverts expressément par ce type de contrat. Elle s'inscrirait également dans la logique des consultations engagées par l'EIOPA sur la gestion des couvertures implicites du risque cyber[65]. En particulier, compte tenu de la difficulté de tracer une frontière claire entre le risque explicite et non explicite, l'EIOPA recommande une approche fondée sur trois aspects : une stratégie et une gouvernance adaptées pour traiter le risque cyber silencieux ; une politique de souscription de produits cyber favorisant les formulations explicites et l'utilisation d'une terminologie cohérente ; enfin, une meilleure prise en compte du risque cyber silencieux en matière de gestion et d'atténuation.

En complément, pourrait être élaboré un guide de place rappelant le cadre juridique et proposant des bonnes pratiques de rédaction aux professionnels. Ce document pourrait notamment traiter de l'objet du contrat dommages aux biens, de la bonne articulation entre la garantie principale et les éventuelles extensions, des définitions – à travers un lexique –, ainsi que des exclusions. Le rappel des règles légales et jurisprudentielles de rédaction, notamment que les clauses d'exclusion doivent être formelles et limitées[66], permettrait de renforcer la sécurité juridique et la lisibilité des contrats. France Assureurs pourrait travailler à l'élaboration d'un tel document, en s'appuyant sur le guide de bonnes pratiques pour la rédaction des contrats RC et DAB en cours de diffusion.

À moyen terme, il pourrait également être envisagé de renforcer l'information de l'assuré pour mentionner explicitement la couverture ou l'absence de garantie du risque cyber dans les contrats professionnels. Une telle évolution se justifierait à la fois par un besoin de sécurité

[62] www.ssi.gouv.fr/entreprise/glossaire
[63] Cass. 2e civ.,17 juin 2021, n° 19-24.467.
[64] En application du IV de l'article L. 612-1 du code monétaire et financier, l'ACPR peut porter à la connaissance du public toute information qu'elle estime nécessaire à l'accomplissement de ses missions. Dans ce cadre, l'ACPR peut procéder à la publication de communiqués de presse.
[65] Consultations publiées en juin 2022 et accessibles via l'URL suivante : https://www.eiopa.europa.eu/media/news/eiopa-consults-its-supervisory-statements-exclusions-insurance-products-arising-systemic_en?source=search
[66] Article L. 113-1 du code des assurances.

juridique mais aussi par l'objectif de protection du consommateur qui doit pouvoir connaître l'étendue de ses garanties. En clarifiant les garanties offertes par chaque contrat d'assurance non-vie (dommages aux biens, responsabilité civile, etc.) cette mesure pourrait mettre fin à l'ambiguïté des couvertures silencieuses. Elle pourrait prendre la forme d'une obligation légale[67] d'information ou d'un engagement de la Place à améliorer l'information fournie, en particulier lors de la souscription. Elle nécessite cependant de définir précisément les faits générateurs cyber concernés et de s'assurer de l'intelligibilité de cette information, en particulier pour les TPE/PME. Si l'option de la norme était privilégiée, cette mesure ne pourrait avoir de portée rétroactive et ne s'appliquerait qu'aux nouveaux contrats, en vertu du principe de sécurité juridique. Un échange préalable approfondi avec la place serait indispensable compte tenu de l'impact de cette mesure sur les systèmes d'information des assureurs, qui devront modifier leurs polices-types, ainsi que sur les réseaux de distribution. De même, une mise en œuvre progressive sera nécessaire.

En complément, il pourrait également être envisagé de mener une évaluation plus fine des garanties implicites sur les contrats commercialisés mais aussi sur le stock de contrats afin d'estimer l'ampleur du phénomène et l'exposition des assureurs au risque cyber.

2.1.2. L'assurabilité des cyber-rançons pourrait être conditionnée au dépôt de plainte afin de renforcer la lutte contre ces pratiques tout en permettant une indemnisation des victimes

Conditionner l'assurabilité du paiement des rançons au dépôt de plainte par la victime permettrait de préserver la viabilité d'entreprises contraintes de s'acquitter de la rançon en dernier recours sans mettre en péril la répression de la cybercriminalité. Le remboursement de la rançon par l'assureur serait subordonné au dépôt de plainte par la victime sous 48 heures. Alors que de nombreuses victimes renoncent à déposer plainte afin de préserver leur image, une telle mesure permettrait de faciliter les investigations en informant systématiquement les autorités judiciaires et en permettant de mieux connaître les méthodes des cybercriminels. Un rançongiciel frappe souvent plusieurs victimes : le recoupement de plaintes et donc d'indices permettrait de faire progresser les investigations. Pour autant, le paiement de la rançon est une option de dernier recours pour préserver l'entreprise. Les conditions de souscription des contrats d'assurance du risque cyber et de tarification devront continuer à inciter les entreprises à adopter des bonnes mesures de protection cyber pour prévenir le risque de sous-investissement des entreprises en matière de sécurité. À moyen terme, il pourrait être envisageable d'organiser un partage de données anonymisées, dans le respect du cadre de protection des données personnelles et du secret de l'enquête, vers l'ANSSI afin d'affiner la connaissance de la menace cyber.

Le risque d'un ciblage accru des entreprises françaises en cas d'assurabilité du paiement des rançons par les cybercriminels est à relativiser car aucun État de l'OCDE n'interdit la couverture de ce risque[68]. Plusieurs d'entre eux ont pris des dispositions visant à renforcer l'information des forces de sécurité, comme au Canada où la victime qui paie une rançon doit le notifier à la police ou en Allemagne, où existe l'obligation pour les assureurs et les assurés d'informer les autorités et de collaborer avec les services de police en cas de demande de rançon.

Une telle disposition est actuellement inscrite dans le projet de loi d'orientation et de programmation du ministère de l'Intérieur (LOPMI) en cours d'examen au Parlement.

En complément, des mesures opérationnelles permettraient d'améliorer la lutte contre les cybercriminels.

[67] Article L. 112-2 du code des assurances.
[68] HAUT COMITE JURIDIQUE DE LA PLACE FINANCIERE DE PARIS, *rapport sur l'assurabilité des risques cyber*, publié en janvier 2022, consulté le 28 juin 2022. URL : https://www.banque-france.fr/sites/default/files/rapport_45_f.pdf

Une coopération accrue entre les assureurs et les forces de sécurité pourrait faciliter la lutte contre la cybercriminalité. Un point de contact unique pourrait être mis en place pour les assureurs à travers une BAL ou des référents identifiés afin de permettre une transmission rapide des éléments pertinents afin que les incidents soient traités par le bon interlocuteur au sein du dispositif national d'assistance aux victimes. Sur le modèle de la déclaration de soupçon transmise à Tracfin, un document type standardisé renseignant les informations essentielles pour les forces de sécurité pourrait être élaboré par l'ANSSI, Tracfin, la DGGN (le commandement de la gendarmerie dans le cyberespace), la DGPN (l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication) et la section J3 du tribunal judiciaire de Paris. À moyen terme, une extension de la plateforme *Thesee*, facilitant le dépôt de plainte en cas d'e-escroquerie pour les particuliers, aux professionnels pourrait également faciliter la mise en place de ces modalités de coopération.

Enfin, les fédérations professionnelles constituent le relai adéquat pour diffuser des mesures de prévention et des bonnes pratiques face aux cyber-rançons. France Assureurs pourrait ainsi rappeler le cadre réglementaire et les mécanismes de signalement mis en place à ses adhérents et diffuser de bonnes pratiques qui pourraient être transmises aux assurés. Surtout, il est indispensable que le paiement de la rançon reste une solution de dernier recours après avoir analysé systématiquement les solutions alternatives. France Assureurs pourra s'appuyer sur la documentation produite par l'ANSSI ou par cybermalveillance.gouv.fr. Des bonnes pratiques en matière de rédaction de clauses peuvent être envisagées, par exemple en rappelant qu'il faut éviter de garantir les rançons payées en cryptoactifs dont la traçabilité est complexe.

Cette organisation pourrait être mise en place rapidement à la suite du vote du projet de loi d'orientation et de programmation du ministère de l'Intérieur. L'ensemble des acteurs impliqués (France Assureurs, le ministère de l'Intérieur, le ministère de l'Économie, des Finances et de la souveraineté industrielle et numérique) pourraient d'ores et déjà engager une déclinaison opérationnelle de ces recommandations sans attendre l'adoption du projet de loi.

2.1.3 Afin de clarifier le cadre juridique, l'inassurabilité des sanctions administratives pourrait être expressément mentionnée dans le code des assurances

La présence persistante de garanties couvrant le risque de sanction dans les polices d'assurance justifie de clarifier le droit pour affirmer explicitement l'inassurabilité des sanctions administratives. Cette clarification inciterait les entreprises à se conformer à leurs obligations issues du RGPD et à investir dans leur cybersécurité.

Compte tenu des risques d'interprétation *a contrario*, il est préconisé d'affirmer un principe général d'inassurabilité des sanctions administratives. En effet, affirmer l'inassurabilité des seules sanctions de la CNIL reconnues dans le III. de l'article 20 de la loi n° 78-17 du 6 janvier 1978 pourrait implicitement laisser accroire que les autres sanctions administratives sont assurables. Une telle option serait source d'insécurité juridique et d'incertitude pour les assureurs et les assurés. Il paraît donc préférable de fixer un principe général affirmant que les conséquences des sanctions à caractère de punition ne sont pas assurables dans le code des assurances[69].

Cette approche présente cependant l'inconvénient de se reposer sur la qualification du juge au cas par cas pour identifier la nature de sanction d'une décision administrative. Or, cette qualification n'est pas évidente pour certains actes administratifs, ce qui est de nature à générer des risques limités d'insécurité juridique.

[69] Une modification de l'article L. 113-1 pourrait être envisagée.

Sous réserve d'un vecteur législatif disponible, l'adoption de cette modification est envisageable en 2023.

2.1.4 Il est recommandé de poursuivre les travaux autour d'une potentielle exclusion de garantie pour cause de cyberguerre dans la mesure où une évolution législative apparaît prématurée

L'inclusion explicite de la cyberguerre dans le régime d'exclusion de garantie pour cause de guerre ne permettrait pas de lever toutes les difficultés, notamment en matière de preuve ou de qualification. Dans son rapport de janvier 2022, le Haut comité juridique de la Place financière de Paris recommande d'actualiser l'article L. 121-8 du code des assurances en définissant la notion de guerre étrangère selon une acception large des moyens utilisés (militaires ou cybernétiques) et des auteurs - dès lors qu'un État opère un contrôle sur l'action en cause ou les individus impliqués. Cette clarification ne permet pas de résoudre toutes les difficultés :

- **La démonstration de l'absence de lien de causalité entre le sinistre et une guerre étrangère par l'assuré est rendue beaucoup plus complexe dans le cas d'une cyberattaque**. Il est plus difficile d'identifier l'origine d'une cyberattaque. Prouver que l'attaque n'est pas imputable à un État étranger ou à un groupe sous son contrôle effectif devient alors très complexe. Les assurés ne sont pas en mesure de procéder à de telles investigations. Cette situation fait reposer une responsabilité forte sur la diplomatie française lorsqu'elle reconnaît ou non l'origine étatique d'une cyberattaque. Cette approche risque également de perturber la conduite des relations diplomatiques, notamment en cas de qualification par une juridiction d'une situation de cyberguerre lors d'un contentieux ;
- **Elle ne permet pas non plus de lever l'insécurité juridique liée à l'indéfinition de la notion de cyberguerre**. Dans la mesure où seuls l'intensité et les effets d'une cyberattaque peuvent la rendre constitutive d'un acte de guerre, l'appréciation d'une possible exclusion s'opère au cas par cas limitant la prévisibilité pour l'entreprise comme pour l'assureur.

Afin de remédier à ces difficultés, il serait opportun d'approfondir les travaux engagés en mettant en place un groupe de travail dédié chargé d'expertiser les implications d'une extension de l'exclusion de garantie à la cyberguerre. Il aurait pour tâche d'identifier des critères de définitions opérationnels permettant de considérer qu'une cyberattaque relève du régime d'exclusion de l'article L. 121-8 du code des assurances. Il pourrait également examiner l'opportunité d'adapter le régime de la preuve. Ce groupe pourrait inclure des représentants de la direction des affaires juridique du ministère des armées, de l'ANSSI, de la direction générale du Trésor, de France Assureurs et de l'AMRAE.

2.2. Une meilleure prise en compte du risque cyber dans le pilotage de l'activité assurantielle ainsi qu'un partage de données accru faciliteraient la mesure du risque

2.2.1. Améliorer la prise en compte du risque cyber dans le pilotage de l'activité assurantielle

a) Afin que les assureurs appréhendent mieux leurs propres expositions au risque opérationnel cyber, le secteur pourrait s'appuyer sur les meilleures pratiques des assureurs les plus avancés dans la démarche, qui incluent d'ores et déjà ce risque au sein de leur ORSA

La prise en compte du risque cyber au sein de l'exercice d'évaluation interne des risques et de la solvabilité (ORSA, *Own Risk and Solvency Assessment*) permettrait de mieux appréhender l'exposition au risque de l'assureur. Défini par l'article 45 de la directive Solvabilité 2, l'ORSA est un processus interne d'évaluation des risques et de la solvabilité effectué par l'assureur. L'objectif de cette évaluation est d'illustrer la capacité de l'assureur à identifier, mesurer et gérer les risques de nature à modifier sa solvabilité ou sa situation financière. C'est un outil stratégique de premier plan qui complète les exigences quantitatives afin que l'entreprise dispose d'un ensemble cohérent d'outils de pilotage de ses risques.

Le rapport ORSA permet ainsi à l'entreprise d'étudier en profondeur l'impact du risque cyber auquel elle est exposée. Bien qu'encadré, cet exercice est appréhendé différemment selon les acteurs : en fonction de leur profil et de leur appétence aux risques propres : certains assureurs ont déjà inclus ce risque au sein de leur rapport ORSA. Un partage des bonnes pratiques et de la méthodologie de ces derniers à l'ensemble du secteur apparait comme un vecteur d'amélioration de la compréhension de ce risque.

Prise en compte du risque cyber dans l'ORSA : bonnes pratiques remontées par les assureurs

1. Approche générale

La prise en compte du risque cyber dans l'ORSA s'appuie, en général, sur une analyse de différents scénarios qui permet d'évaluer les risques de l'ensemble de l'entreprise et d'en estimer l'impact cumulé. L'objectif est de développer des scénarios tout à la fois sévères et plausibles ne découlant pas uniquement de données historiques et d'adopter une vision prospective. Les évènements qui remettraient en cause la viabilité du modèle d'activité peuvent également être pris en compte (tests de résistance inversés). Les hypothèses de choc s'appuient autant sur les données disponibles que sur l'analyse et le jugement d'experts.

L'impact de ces scénarios ou d'une combinaison de ces scenarios sur la solvabilité de l'assureur (ratio fonds propre/capital de solvabilité requis) ainsi qu'une analyse qualitative des scenarios est ensuite présentée et détaillée dans le rapport ORSA. Ces scenarios et leurs impacts peuvent également tenir compte d'effets supplémentaires indirects, en fonction des pratiques de différents acteurs (détérioration de la sinistralité relative aux produits cyber, aux lignes financières, paiement de rançon éventuelles ou d'amendes réglementaires, atteinte à la réputation, etc…)

Il est à noter que l'analyse sollicite tant la collecte de données internes d'exposition de l'entreprise que des données externes.

2. Définition des scénarios

Pour construire les hypothèses et trajectoires de stress, des scénarios de stress réalistes (*Realistic Disaster Scenario* ou RDS) sont développés. Il peut s'agir, par exemple, d'une attaque de très grande ampleur, à l'encontre de sites de e-commerce assurés, entraînant une interruption d'activité, d'une violation des données impliquant des réclamations en responsabilité civile, d'une défaillance majeure d'un grand fournisseur de cloud ou d'une attaque sur une entreprise technologique majeure dont plusieurs industriels sont dépendants, en fonction du profil de risques de l'entreprise et des expositions existantes.

Ces scénarios peuvent être calibrés à l'aide de données, comportant les données marché, et peuvent être alimentés par des éléments académiques disponibles (i.e. Cambridge University Mass Vulnerability Scenario). Ils tiennent compte des pertes liées aux couvertures cyber affirmatives, mais aussi silencieuses (cf. 1.2.1 a)) incluses dans d'autres lignes de produit que cyber. Ils évaluent l'impact potentiel de ces risques sur l'ensemble de l'entreprise afin d'en comprendre le potentiel cumulatif en considérant également les impacts sur la souscription (risque d'assurance), l'investissement (risque de marché) et les opérations (risque opérationnel). Ces scénarios sont conçus pour tester les impacts prudentiels en termes de fonds propres et de liquidité. Les assureurs interrogés revoient régulièrement ces scénarios (en général annuellement), au travers d'une gouvernance dédiée.

3. Conséquences de l'analyse

L'intégration du risque cyber dans l'ORSA, peut nourrir le plan de gouvernance de l'entreprise grâce :

- au suivi régulier des expositions au risque cyber présenté au comité des risques ;

- à la gestion des expositions au risque en définissant des limites de souscription en adéquation avec l'appétit au risque ;

- à l'évaluation annuelle des risques opérationnels via des scénarios d'interruption majeure d'opérations suite à une cyberattaque.

Elle peut également mener, le cas échéant, à l'évolution du modèle interne de calcul du capital de solvabilité requis (SCR) en y incluant le risque cyber (par exemple dans les risques de primes, de catastrophe d'origine humaine ou opérationnelle).

Par ailleurs et de façon complémentaire à l'ORSA, des discussions sont en cours au niveau européen concernant l'élaboration de tests de résistance (*stress tests*) cyber. Début 2022, l'EIOPA[70] a présenté une feuille de route pour l'élaboration de principes méthodologiques de tests de résistance en assurance portant sur le risque cyber, à l'instar de ce qui a été fait sur d'autres risques. L'objectif de tels travaux est de tester la résistance des entreprises d'assurance face à la matérialisation du risque cyber.

[70] *European Insurance and Occupational Pensions Authority* (EIOPA) : Autorité européenne des assurances et des pensions professionnelles.

b) Pour améliorer le pilotage économique et réglementaire des passifs exposés au risque cyber, il est recommandé de créer une catégorie ministérielle d'assurance dans le code des assurances dédiée au risque cyber. À moyen terme, une évolution de la réglementation européenne et notamment la classification en lignes d'activité devrait être envisagée.

La difficulté à caractériser le risque cyber, qui prend des formes diverses et qui touche tant les activités des entreprises tous secteurs confondus que celles des particuliers, appelle un meilleur suivi.

Aujourd'hui, les contrats et garanties cyber ne forment pas une catégorie identifiée dans la réglementation : ils peuvent relever de la catégorie dommages aux biens, mais aussi de la responsabilité civile ou des pertes pécuniaires. Sans une catégorisation claire, les *reportings* réglementaires ne permettent pas de retracer l'activité de l'assurance du risque cyber et d'assurer un suivi indispensable au pilotage du risque. La détermination des montants de prestations, de la sinistralité ou du provisionnement sont rendus plus complexes en l'absence d'identification claire du risque. Les garanties cyber sont diluées au sein d'autres garanties.

Afin de combler cette lacune d'information, une première piste est la création d'une nouvelle catégorie ministérielle d'assurance dédiée[71]. Les catégories ministérielles, définies par arrêté aux articles A. 344-2 du code des assurances, A.114-1 du code de la mutualité et A.931-11-10 du code de la sécurité sociale, sont une spécificité de la comptabilité et du *reporting* français. L'ajout d'une catégorie dédiée permettrait d'obtenir des données comptables et statistiques en matière de risques cyber par le biais des états nationaux spécifiques (ENS), compléments du *reporting* Solvabilité 2. En outre, les autorités de contrôle disposeront d'un ensemble de données fiables et normalisées sur le risque cyber assuré, à l'instar des autres risques assurés, ceci permettant un meilleur suivi.

En tout état de cause, une catégorie dédiée à l'assurance du risque cyber ne serait pleinement opérationnelle qu'à la condition de remédier aux garanties implicites, lesquelles ont pour conséquence qu'un risque cyber peut être couvert sans être nommé, dès lors que les dommages causés font l'objet d'une couverture d'assurance sans que soit explicitement exclue l'origine cyber des dommages. Par conséquent, les portions de primes et les sinistres se rattachant à ces garanties cyber ne sont pas toujours identifiés dans les bases de données des assureurs. La clarification préalable des clauses contractuelles aux fins de garantir expressément de tels risques apparaîtrait donc comme un prérequis indispensable à une telle recommandation.

L'EIOPA a publié le 31 mars 2022 les projets de modification des normes techniques d'exécution (*Implementing Technical Standards*2 015/2450 et 2015/2452)[72] **établissant des obligations de déclaration QRT** (*Quantitative Reporting Templates*) **dans le cadre de Solvabilité 2**. Ces amendements poursuivent différents objectifs, dont l'un concerne la création d'un *reporting* sur le risque cyber : un nouveau *template* S.14.03 intitulé *cyber underwriting risk* regrouperait sur les informations de cette activité, notamment les risques inclus par la couverture, les sommes assurées et réassurées, les primes collectées et les sinistres. Ce nouveau QRT permettra d'obtenir des informations sur le risque cyber dans la métrique Solvabilité 2 qui seront un complément indispensable à l'approche comptable des ENS français.

---

[71] La création d'une branche cyber fait partie des préconisations du rapport du Groupe d'Étude Assurance de l'Assemblée Nationale du 13 octobre 2021 présidé par la Députée Valéria FAURE-MUNTIAN (URL : https://www.lassuranceenmouvement.com/wp-content/uploads/2021/10/Rapport_La-Cyber-assurance_Valeria_Faure-Muntian_13102021.pdf), de la note de position de l'Association des professionnels de la réassurance en France (APREF) « Assurance et réassurance du risque Cyber » de décembre 2021 (URL : https://www.apref.org/wp-content/uploads/2022/02/2021-12-03-Apref-Note-de-position-Cyber-VF.pdf) ainsi que l'avis du Conseil économique, social et environnemental intitulé « Climat, cyber, pandémie : le modèle assurantiel français mis au défi des risques systémiques » d'avril 2022 (URL : https://www.lecese.fr/travaux-publies/climat-cyber-pandemie-le-modele-assurantiel-francais-mis-au-defi-des-risques-systemiques).

[72] EIOPA, *Draft Amended Implementing Technical Standards (ITS) on supervisory reporting and disclosure*, mis en ligne le 31 mars 2022 et consulté le 28 juin 2022. URL : https://www.eiopa.europa.eu/document-library/technical-standard/draft-amended-implementing-technical-standards-its-supervisory_en

Il s'appliquerait aux entreprises ayant une activité d'assurance du risque cyber représentant au minimum 5 millions d'euros de chiffre d'affaires, 5 % des primes d'assurance non-vie, ou 3 % des contrats d'assurance non-vie et entrerait en vigueur à partir du 31 décembre 2023. La création d'un état de *reporting* spécifique peut permettre de mener à la création d'une ligne d'activité dédiée au sein du règlement délégué à Solvabilité 2, préalable indispensable à la prise en compte systématique du risque cyber dans le calcul des exigences en capital.

La création d'une catégorie ministérielle et d'une ligne d'activité spécifique pourrait être complétée par la création d'une branche dédiée à l'assurance du risque cyber au niveau européen[73]. En étendant ainsi la liste européenne des branches, l'exercice de cette activité par tout assureur européen serait subordonné à un agrément spécifique. Les garanties cyber ne pourraient être commercialisées qu'après autorisation du superviseur qui s'assurerait de la solidité du plan d'activité de l'entreprise souhaitant les proposer. Cette obligation renforcerait la qualité et la soutenabilité des couvertures cyber.

2.2.2 Répondre à la problématique du manque de données cyber

a) Une bonne modélisation du risque cyber doit reposer sur une méthodologie rigoureuse. Compte tenu du temps nécessaire à la constitution de bases de données suffisantes, un ratio global de solvabilité confortable constitue un préalable.

La détention d'une base de données cyber ainsi que la mise en œuvre d'une bonne modélisation sont un prérequis pour que les assureurs puissent faire une projection du coût économique de leurs engagements à assurer les clients contre ce risque. Il est ainsi essentiel de connaître les réalisations de ce risque observées dans le passé et, si possible, recourir à des avis d'experts sur son évolution probable.

Disposer d'une base de données cyber de qualité présente plusieurs bénéfices pour appréhender au mieux ce risque. Elle permet, tout d'abord, de réduire les incertitudes liées aux projections statistiques actuarielles et de mieux estimer le risque sous-jacent ce qui permet aux assureurs de provisionner et tarifer les garanties en conséquence. Elle permet également de mieux anticiper l'évolution du risque et de calibrer plus finement le montant des futures primes et des provisions. Une segmentation des entreprises peut également être mise en place selon des objectifs pertinents d'exposition au risque (chiffre d'affaires, nombre de salariés, secteur d'activité, critère de qualité de la sécurité informatique) en catégories assez homogènes de coûts d'impact du risque. Ceci permettant une meilleure mutualisation du risque entre les assurés. L'accès à la donnée induit également une meilleure quantification de l'impact des bonnes pratiques des assurés ce qui permet de dimensionner des réductions de primes pour les assurés les plus vertueux. Il peut s'agir, par exemple, d'une entreprise qui investirait dans des équipements ou de la formation en cybersécurité. L'assureur peut également mettre en œuvre des stratégies de prévention à l'échelle d'un portefeuille.

L'Institut des actuaires rappelle les bases d'une bonne identification des données à prendre en compte et de leur structuration en vue d'une modélisation fiable du risque cyber, intégrant le contexte et l'impact des incidents. Cette méthodologie s'appuie sur l'identification de trois blocs :

- bloc 1 : données relatives à **la description du sinistre** (coût de l'incident, nature de l'attaque, etc.) ;
- bloc 2 : données relatives à **l'accumulation**. Il s'agit des informations permettant de relier un incident à un groupe d'incidents ou son lien avec d'autres risques (déclenchement

[73] La liste des branches et sous-branches d'agrément telle que prévue par l'article R. 321-1 du Code des assurances est, ainsi, issue de la transposition de l'annexe I (branches non vie) et de l'annexe II (branches vie) de la Directive n° 2009/138 du 25 novembre 2009 dite Solvabilité 2.

d'autres garanties comme la perte d'exploitation, etc.). Elles permettent également de mettre en exergue les « chaînes de contamination » ;
- bloc 3 : informations sur **la victime**. Elles permettent de relier les dommages à un profil particulier.

L'institut insiste sur la nécessité de recourir à une description non agrégée de l'incident (c'est-à-dire victime par victime). Pour éviter l'écueil d'une analyse purement descriptive, il est également important de corréler les trois blocs entre eux. Ceci permet de relier les comportements à une distribution des pertes potentielles.

Par ailleurs, l'analyse actuarielle ne peut se contenter d'informations purement techniques. Les informations demandées correspondent, d'une part, à des variables dont l'assureur peut avoir connaissance au sein de son portefeuille (permettant la comparaison de celui-ci aux sinistrés de la base de référence) et, d'autre part, à des variables sur lesquelles l'assureur peut agir dans le cadre de sa stratégie de prévention (niveau de sécurité, « hygiène informatique », contrats d'audit et d'assistance, *etc.*).

Il souligne, enfin, l'importance de l'anonymisation de ces données. En effet, les données collectées sont potentiellement des données très sensibles qu'il est nécessaire de protéger. À cette fin, il est possible de catégoriser certaines variables afin de rendre la réidentification plus difficile. Des techniques existantes et sures, utilisant uniquement des données cryptées, permettent d'effectuer des analyses en partageant ces données et en ayant accès uniquement aux résultats sans que l'utilisateur puisse avoir un accès direct aux données. Plusieurs *start-ups* offrent des solutions de ce type et travaillent d'ores et déjà avec certains assureurs.

b) L'usage des méthodes alternatives pour pallier, dans un premier temps, le manque de données peut être envisagé

Les assureurs qui disposent de peu données et d'un ratio global de solvabilité confortable, pourront recourir à des méthodes innovantes, moins fiables, mais s'adaptant de façon continue à l'aide des données nombreuses du moment.

Les approches bayésiennes sont particulièrement intéressantes pour modéliser les risques émergents et répondre au déficit de données. Elles consistent à intégrer une connaissance préliminaire (« *a priori* ») à des données d'expérience. Les actuaires mobilisent ainsi d'autres études ou analyses qui complètent l'information et tendent à avoir une vision holistique du risque. Ces analyses permettent d'améliorer la maitrise et l'anticipation du risque et peuvent donner au marché français un avantage compétitif dans le développement d'une offre d'assurance du risque cyber. Elles présentent également l'intérêt de rassurer les assureurs dans la prise en charge de ce risque. Ces logiques sont déjà utilisées avec succès en assurance comme, par exemple, dans les tables de mortalités réglementaires.

Cependant, ces méthodes nécessitent une bonne connaissance de l' « *a priori* » sous peine de devenir contre-productives. Ces approches sont utiles dans une phase de démarrage d'activité ou pour prendre en compte une évolution récente du risque comme cela est le cas pour le risque cyber. Toutefois elles ne peuvent fonctionner que si elles reposent sur une analyse scientifique rigoureuse et ne suppriment pas la nécessité de disposer de solides bases de données, notamment à échelle macroscopique (qui dépassent le portefeuille de l'assureur).

Le recours à l'intelligence artificielle (IA) peut également être une solution pour aider à la modélisation du risque cyber. La startup Citalid a ainsi développé un modèle réunissant trois sources de données : les modèles actuariels, l'expertise cyber et la « *cyber threat intelligence* ». Cette dernière source vise à utiliser l'intelligence artificielle, pour rechercher les données cyber accessibles en sources ouvertes (publiées par les autorités, données académiques…). L'usage de l'intelligence artificielle, nourrissant l'inférence bayésienne, permet une modélisation du risque avec peu de données, s'améliore à mesure que les données affluent et évolue à mesure que les données changent.

Il est cependant à souligner que si ces techniques innovantes apparaissent très utiles, elles ne sauraient à elles-seules résoudre l'ensemble des questions posées par le manque de données. Il faut en effet rappeler que l'IA, bien loin de compenser l'absence de données, a besoin d'une quantité très importante d'information pour fonctionner correctement. En revanche, l'IA peut travailler à partir de données non structurées, et en dégager une structure difficile à percevoir sans la machine IA. Ces techniques paraissent donc très prometteuses en vue d'extraire certains facteurs de risque, notamment à partir des flux internet ; leur déploiement efficace pourrait représenter un élément de compétitivité pour le marché français.
Néanmoins, ces méthodes ne semblent pas les plus adaptées pour anticiper les vulnérabilités humaines, et surtout elles ne permettent pas de quantifier les impacts économiques sans le soutien de données structurées et fiables sur les coûts des incidents.

Ces méthodes alternatives et leur appropriation par les acteurs français de l'assurance du risque cyber, permettraient au marché français de développer une expertise cyber pointue le dotant d'un avantage compétitif certain.

c) Pour permettre la construction d'une base de données du risque cyber fiable favorisant le développement d'une offre assurantielle de long terme, une mise en commun des données est nécessaire.

L'accès de tous les assureurs à un ensemble des données permettrait d'aller plus vite dans la connaissance du risque, de positionner chaque portefeuille de contrats par rapport à l'ensemble du marché à assurer et d'élargir l'offre et la mutualisation. Ceci constitue les conditions de tarifs plus abordables et plus adaptés, tout en apportant plus de capacité de couverture.

La constitution d'une base de données partagée, issue d'une mutualisation entre détenteurs de données de sinistralité cyber, apparait comme la meilleure solution pour pallier le déficit de données. Cette solution, qui pourrait être mise en œuvre à un horizon plus long, s'appuierait sur un partage de données, via une structure *ad hoc* de type partenariat public/privé. Ce tiers de confiance, garant de la qualité de la donnée, devrait s'attacher à la confidentialité des données recueillies.

La donnée cyber présente comme caractéristique d'être collectée et fragmentée entre différents acteurs (public et privé). Chaque assureur collecte d'importantes masses de données relatives à la sinistralité cyber. Cependant, ces données se limitent à la sinistralité constatée par chaque assureur au sein de son portefeuille. Il serait ainsi pertinent d'enrichir ces données internes par les données de sinistralité des autres acteurs afin d'analyser plus finement ce risque et piloter au mieux l'activité assurantielle. Les pouvoirs publics peuvent également disposer de données de sinistralité (ANSSI, le GIP ACYMA, les autorités judiciaires, la police, la gendarmerie, la CNIL…).

Par principe, la politique de la concurrence interdit le partage d'informations jugée favorable aux collusions et donc à un mauvais fonctionnement du marché. Dans le secteur de l'assurance, l'information sur les sinistres passés est un actif essentiel à la stratégie de souscription et de modulation des primes**. En revanche, un partage de ces informations favorise, de manière globale et sectorielle, l'efficacité de ces stratégies.** Ainsi, la politique de concurrence admet ces partages d'information qui doit cependant être agrégée et rendue anonyme. Le pilotage de ce partage par un tiers de confiance permettrait ainsi ce partage dans le respect des règles de concurrence. Ce partage d'information dans le secteur de l'assurance peut même stimuler la concurrence. Se faisant, il lève les barrières à l'entrée et favorise la concurrence entre les acteurs. En outre, le partage permet aux nouveaux acteurs d'être plus résilients. Dans un rapport dédié, l'OCDE indique que le partage d'information sur les sinistres cyber permettrait effectivement d'accroitre la concurrence, sur les marchés pour l'instant dominés par quelques grands acteurs[74]. Ce partage se justifie d'autant plus qu'il s'agit d'un risque nouveau ou moins fréquent, et donc pour lequel

[74] OECD, *Enhancing the Availability of Data for Cyber Insurance Underwriting, The Role of Public Policy and Regulation,* publié en 2021 et consulté le 28/06/2022. URL: www.oecd.org/finance/insurance/Enhancing-the-Availability-of-Data-for-Cyber-Insurance-Underwriting.pdf

l'information est manquante. Il est à noter que ce type d'initiative a déjà été mise en place, notamment pour le risque catastrophe naturelle. En Australie, les acteurs de marché membres du *Insurance Council of Australia* se sont organisés pour collecter et publier des données agrégées sur les sinistres et pertes en catastrophes naturelles. En France, les assureurs transmettent ces données agrégées liées aux catastrophes naturelles à l'Observatoire national des risques naturels[75].

Les données recueillies par cette plateforme pourraient être utilisées pour différentes finalités. Les pouvoirs publics pourront, tout d'abord, dimensionner des politiques publiques adaptées en objectivant le phénomène. Ces données pourront également être utilisées par les acteurs de marché, tels que les assureurs, afin de proposer des offres d'assurance du risque cyber adaptées à l'état de la menace. Ceci permettrait à la filière française de l'assurance de se doter d'un avantage compétitif et serait facteur d'innovations.

Concernant les modalités opérationnelles, ce partage d'information pourrait se faire dans le cadre du projet d'un Observatoire des incidents cyber, placé sous l'égide de l'ANSSI, co-porté avec le GIP ACYMA, et dont les travaux devraient aboutir au premier trimestre 2023. Il pourrait réunir acteurs de marché (assureurs, réassureurs), pouvoirs publics et experts du monde académique. Parmi les enjeux auxquels devra répondre ce dispositif figurent la confidentialité des données, leurs modalités de partage ainsi que les incitations à partager les données. En effet, les données pourraient être diffusées pour servir à la création de politiques publiques dédiées, ce qui pose la question de leur confidentialité et des modalités d'anonymisation. Elles pourraient également être utilisées par les assureurs ainsi que par d'autres parties prenantes du monde de l'Enseignement Supérieur et de la Recherche pour connaître au mieux le risque et construire leur offre d'assurance. Enfin, des incitations à destination des structures qui partagent leurs données devront également être mises en œuvre (partage régulier de données collectées avec exigences de qualité, *etc.*).

Pour que cet observatoire réponde aux objectifs de sécurité informatique, de protection financière et résilience des entreprises (par la mutualisation de leurs risques cyber) et de fourniture de données adéquates aux assureurs, il est nécessaire que sa conception tienne compte des besoins actuariels, de pilotage et de solvabilité des assureurs.

La mise en place d'une telle plateforme pourrait s'inscrire dans les actions de la stratégie nationale d'accélération pour la cybersécurité, annoncée le 22 février 2021 par le Président de la République. Le dispositif visant à favoriser la mutualisation des données d'intérêt cyber pourrait en particulier être mobilisé.

[75] Voir l'Observatoire National des Risques Naturels : https://www.georisques.gouv.fr/

2.3. Un partage du risque plus efficace, impliquant des efforts de résilience accrus des entreprises et l'adoption de méthodes actuarielles innovantes, permettrait de viabiliser l'offre d'assurance du risque cyber

2.3.1. Face à la réduction des couvertures, la promotion de l'auto-assurance par la constitution de captives de réassurance peut constituer une solution pour les entreprises confrontées au risque cyber

Une provision spécifiquement dédiée aux captives de réassurance, facilitant la mutualisation des pertes sur un temps long, inciterait les entreprises à en constituer. Dans la mesure où les captives n'assurent que les risques portés par les entreprises du groupe – potentiellement corrélés –, il est nécessaire de prévoir une gestion inter temporelle du risque en permettant l'accumulation de réserves pour faire face à des variations fortes de la sinistralité selon les années. Ainsi, cette provision doit donner la possibilité aux captives de réassurance de provisionner en franchise d'impôt les excédents d'une année pour les utiliser lors d'exercices ultérieurs afin de lisser leurs bénéfices dans le temps et de se couvrir contre des risques à long terme. À cette fin, les paramètres de la provision pour égalisation doivent être adaptés :

- La couverture de cette provision ne se limiterait pas seulement aux risques exceptionnels mais serait étendue à l'ensemble des risques éligibles, notamment à tous les sinistres ayant une origine cyber ;
- Les plafonds de dotations, annuelle et globale, seraient élevés pour tenir compte du contexte concurrentiel international ;
- Les dotations et les reprises seraient fongibles pour tous les risques concernés ;
- Le délai de déductibilité à l'impôt sur les sociétés serait aligné sur l'horizon de gestion des captives. Au-delà, la provision serait reprise en l'absence de sinistre.

Ces évolutions supposent pourraient intervenir dès 2023 après adaptation du code général des impôts et du code des assurances.

Enfin, la mise en place de cette provision peut s'accompagner de mesures supplémentaires facilitant la création et la gestion des captives de réassurance. Depuis juin 2021, ces entités sont dispensées de la remise d'une dizaine d'états nationaux spécifiques grâce à la modification de l'instruction[76] dédiée de l'APCR. En outre, dans le cadre de la revue 2020 de la directive Solvabilité 2, des allègements prévus par le nouveau statut des petites entreprises non-complexes (*small and non-complex*) doivent s'appliquer spécifiquement aux captives de réassurance.

À moyen terme, le développement des captives par compartiment permettrait à des entreprises aux ressources plus limitées d'accéder à une forme de mutualisation de gestion de captives. Les captives par compartiment permettent à différentes entreprises d'utiliser une structure commune sans pour autant mutualiser leur risque. Les démarches de création d'une captive peuvent être complexes pour des entreprises de petite taille, peu au fait des procédures à suivre. La préexistence d'une structure administrative permettrait aux petites entreprises de ne se focaliser que sur la question sous-jacente la plus importante : la nécessité de se prémunir contre les risques auxquels elles sont exposées. Les captives par compartiment permettraient donc à des petites entreprises d'accéder plus facilement à ces solutions d'auto-assurance en réduisant les coûts fixes de constitution d'une captive de réassurance. Le développement d'un écosystème favorable aux captives pourrait faciliter l'émergence de telles structures.

[76] IV de l'article 2 de l'instruction n° 2016-I-16 en date du 27 juin 2016 modifiée par l'instruction n°2021-I-07 du 18 juin 2021.

Certaines entreprises envisagent par ailleurs de mettre en place des mécanismes de mutualisation du risque. Ces entreprises de secteurs et d'activités diverses se regrouperaient pour créer des mutuelles afin de mettre en œuvre, entre elles, un mécanisme de solidarité financière. Le fonctionnement de l'entité ainsi créée ne diffèrerait pas de celui d'une mutuelle classique. Chaque entreprise définirait ensuite le programme d'assurance qu'elle souhaite que la mutuelle lui fournisse. En cas de sinistre, la mutuelle dédommagerait le sociétaire concerné et en cas d'insuffisance de fonds, un appel de cotisation exceptionnel serait effectué.

2.3.2 L'adoption de pratiques innovantes par les assureurs, comme l'assurance paramétrique, pourrait faciliter la couverture du risque cyber

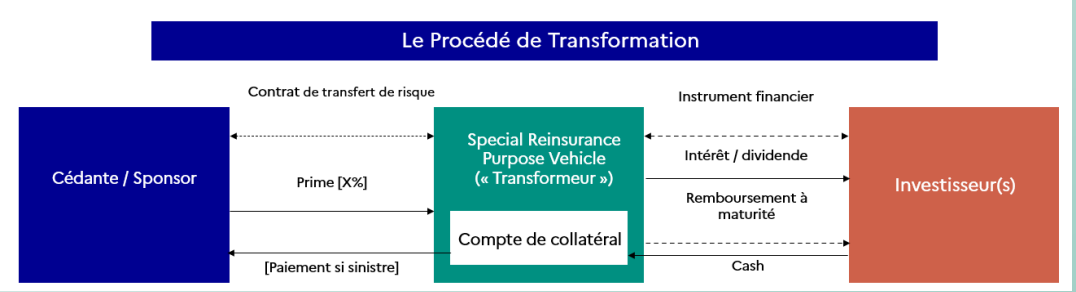
a) Bien que prometteur, le recours aux marchés financiers par les assureurs pour libérer de la capacité de couverture n'est pas envisageable à court terme

Le transfert du risque aux marchés de capitaux par les assureurs peut constituer un moyen de libérer de la capacité assurantielle pour couvrir davantage d'entreprises exposées au risque cyber. La profondeur des marchés financiers peut être exploitée pour transférer le risque, notamment des risques extrêmes, à travers des mécanismes de titrisation : les *insurance linked securities*.

LES *INSURANCE-LINKED SECURITIES*

Issus de la titrisation de contrats d'assurance, les « *Insurance-Linked Securities* » (ILS) sont des titres financiers dont la valeur est déterminée par la survenance d'un sinistre.

Ces titres peuvent être émis par une société *ad hoc* (*special vehicule purpose* - SPV) : cette entité conclut un accord de réassurance avec un sponsor (l'assureur) et perçoit les primes du sponsor en échange du transfert du risque. Le SPV émet ensuite des titres à l'intention des investisseurs et reçoit en retour des montants en principal, déposés sur un compte de garantie. L'investisseur porte le risque : en cas de survenance du sinistre, l'investisseur perd une partie ou la totalité du capital au profit du sponsor qui peut alors indemniser le dommage.



Ce procédé s'est particulièrement développé à partir des années 1990 pour la gestion des catastrophes naturelles à travers les *Catastrophe Bonds* (ou *cat bonds*). Ils concernent la couverture de risques liés à des catastrophes naturelles : le coupon ou le prix de remboursement de ce type d'obligation est fortement réduit en cas de catastrophe.

Les ILS permettent également aux investisseurs de diversifier leur portefeuille, facilitent la prise en charge de risques extrêmes et constituent une alternative à la réassurance. Pour les investisseurs, dans la mesure où les sinistres ne sont en principe pas corrélés aux variations des

marchés financiers les ILS diversifient leur portefeuille ou constituent un instrument de couverture. Pour les assureurs, ce mécanisme complète les offres classiques de réassurance et permet de libérer de la capacité. Pour l'assuré, il facilite la prise en charge de risques extrêmes, présents en matière cyber, en permettant de s'appuyer sur la profondeur des marchés financiers. Ainsi, ces raisons ont poussé CCR Re à lancer, en 2019, le premier ILS français à travers le fonds FCT 157 portant notamment des risques de catastrophe immobilière.

Cependant, la transposition de ce type de solution au risque cyber est complexe en raison de ses caractéristiques, du manque de données ainsi que de la difficulté à définir des indices pertinents. La plus faible diversification géographique ou l'existence d'une corrélation entre cyberattaque et variation des marchés de capitaux sont de nature à freiner l'appétence des investisseurs pour les ILS cyber. De même, la duration d'un ILS cyber serait relativement élevée par rapport à un *cat bond* dans la mesure où le risque cyber inclut une composante responsabilité civile, qui implique un délai plus long entre le sinistre et l'indemnisation. Le manque de recul et de fiabilité des données de modélisation ainsi que la difficulté à définir des paramètres de déclenchement de garantie en matière cyber constituent également des obstacles. Aujourd'hui, très peu de capacités sont déployées sur ce risque par les marchés financiers.

Le recours aux marchés financiers pour porter une partie du risque cyber est donc difficilement envisageable à court terme. Cependant, les efforts de partage des données, de modélisation et de formation sont de nature à favoriser l'émergence d'une offre d'ILS cyber à moyen terme.

b) Dans un contexte de durcissement des conditions d'assurance, l'assurance paramétrique peut constituer un outil utile pour permettre la couverture d'une partie du risque cyber.

À la différence de l'assurance dommage traditionnelle qui indemnise l'assuré en fonction des pertes effectivement subies, **les garanties paramétriques ou indicielles permettent le versement automatique d'une prestation établie en fonction d'un indice mesurable automatiquement dès que la valeur de cet indice franchit le seuil de déclenchement de la couverture.** Défini dans le contrat, l'indice de référence est lié à la perte et facilement mesurable. La garantie paramétrique peut constituer un levier de simplification : la survenance du sinistre et le niveau d'indemnisation sont déterminés par le franchissement d'un indicateur. Le recours à un expert n'est pas nécessaire. Le montant d'indemnisation est connu de façon quasi instantanée et le déclenchement automatique des garanties raccourcit les délais de paiement. Ce type de garantie s'est particulièrement développée dans le monde pour les catastrophes naturelles : la vitesse du vent ou encore le niveau des précipitations font partie des indices utilisés.

L'assurance paramétrique constituerait donc un outil potentiellement adapté au risque cyber pour libérer des capacités et inciter les assureurs à offrir des couvertures. Dans la mesure où la plupart des sinistres cyber sont de faible intensité, la prise en charge par une assurance simplifiée permettrait d'indemniser de manière adéquate l'essentiel des victimes de cyberattaques. Enfin, à moyen terme, la diffusion de produits paramétriques faciliterait la titrisation sous forme d'ILS. La durée d'interruption d'accès à un service cloud ou à un site de vente en ligne font partie des types d'indices actuellement à l'étude par des professionnels du secteur pour construire une offre d'assurance paramétrique cyber.

Afin d'aider à l'identification de paramètres pertinents pour le risque cyber, les synergies entre acteurs publics et privés sont à encourager. Pour un fonctionnement optimal, le paramètre doit être disponible, facilement mesurable et suffisamment corrélé au risque assuré. L'assuré doit également le percevoir comme une approximation satisfaisante du risque contre lequel il souhaite se protéger. Alors que plusieurs acteurs, notamment Descartes Underwriting, ont déjà engagé des efforts de recherche et développement pour identifier des indicateurs pertinents, un partage de

données accru faciliterait l'émergence d'une offre de garanties paramétriques[77]. Un groupe de travail incluant notamment l'institut des actuaires, l'ANSSI et des entreprises développant ce type de solution permettrait de définir les jeux de données nécessaires à la constitution de paramètres pour l'assurance du risque cyber et travaillerait à favoriser leur ouverture en source ouverte. Par ailleurs, la sensibilisation des acteurs de la place à ce type de garantie par les fédérations de professionnels peut également constituer une piste pour diffuser ces pratiques.

Cependant, l'assurance paramétrique ne peut traiter l'intégralité du risque cyber dans la mesure où elle ne permet pas de gérer les pertes en cas de sinistre extrême ni de traiter certaines composantes du risque. L'assurance paramétrique ne permet pas une bonne couverture des sinistres de montant élevé. De plus, le cyber regroupe plusieurs types de garanties et certaines demandent une expertise humaine, en particulier les garanties liées à la responsabilité civile. Par ailleurs, il est nécessaire de définir une offre compatible avec le cadre juridique français, notamment au regard du principe indemnitaire[78] en assurance de dommages aux biens selon lequel le montant de l'indemnité ne peut excéder le montant de la valeur de la chose assurée au moment du sinistre. De même, il existe un risque juridique concernant la qualification d'opération d'assurance si l'objet du contrat n'est pas suffisamment lié au dommage subi par l'assuré. Enfin, le déploiement à moyen terme d'une offre d'assurance paramétrique nécessitera des efforts de formation des réseaux de distribution pour qu'ils puissent conseiller au mieux les assurés sur ce type de produit. Ainsi, l'assurance paramétrique ne peut constituer qu'un outil parmi d'autres pour couvrir le risque cyber.

2.4. Un accroissement des efforts de sensibilisation des entreprises et un accompagnement renforcé stimulerait la demande d'assurance du risque cyber

2.4.1. Des efforts de sensibilisation accrus pour les entreprises, en particulier à destination des TPE/PME, pourraient réduire la sous-estimation du risque cyber

a) Améliorer la mesure du niveau de maturité cyber des entreprises faciliterait l'accès à l'assurance du risque cyber et les efforts des entreprises pour améliorer leur résilience

La diffusion de standards communs de cybersécurité inciterait les entreprises à renforcer leur résilience cyber. En étant utilisé dans l'appréciation du risque par les assureurs, ces référentiels conduiraient les entreprises à investir pour mieux maîtriser leur exposition au risque afin de mieux se protéger et de plus facilement transférer ses risques à son assureur. L'identification du niveau de maturité cyber des entreprises constitue un levier pour améliorer leur cybersécurité en mettant en lumière des besoins et des marges de progression. La définition de ce modèle de maturité pourrait être déclinée en référentiels de sécurité, utilisés dans la tarification des assureurs. La définition de standards de cybersécurité adaptés au nouveau cadre juridique européen, notamment la directive NIS 2[79] constitue enfin un enjeu de souveraineté dans un contexte où les référentiels américains[80] pourraient s'imposer.

Les acteurs du secteur, et notamment l'AMRAE, proposent ainsi de travailler à la mise en place d'un modèle de maturité cyber décliné en référentiels selon la taille et l'activité des entreprises.

[77] Par exemple, l'accès à des données sur des interruptions du réseau électrique pourrait être utile selon les entreprises d'assurance qui travaillent sur ce type d'offre.
[78] Article L. 121-1 du code des assurances.
[79] *Network Information Security.*
[80] *Bitsight* ou *Security Scorecards*

Ces référentiels seraient adaptés à différents niveaux de maturité (basique, intermédiaire, avancé) et à la structure organisationnelle de l'entreprise. L'évolution rapide de la menace cyber suppose de faire évoluer régulièrement les référentiels. L'évaluation de l'entreprise pourrait reposer sur des auditeurs qui attribueraient une note à l'autoévaluation réalisée par l'entreprise. Ce modèle de maturité devrait être aligné avec la directive NIS 2 dont l'entrée en vigueur est prévue au second semestre 2022.

Cependant, la reconnaissance de ces référentiels par les assureurs est nécessaire pour qu'ils constituent un véritable levier d'incitation pour les entreprises à renforcer leur cybersécurité. Pour atteindre cet objectif, des représentants du secteur de l'assurance devront être associés à la définition des référentiels. **Il apparait également nécessaire de veiller autant que possible à ne pas alourdir la charge administrative des entreprises**. En ce sens, il ne paraît donc pas opportun de conditionner l'assurance du risque cyber à l'évaluation par le référentiel, dans la mesure où cela pourrait se traduire par une augmentation du coût de l'assurance du risque cyber. Les entreprises peu risquées pourraient ne pas s'assurer, accroissant ainsi le risque d'anti sélection.

À court terme, un travail sur l'harmonisation des questionnaires de sécurité permettrait de limiter la complexité administrative pour les entreprises facilitant ainsi l'accès à l'assurance du risque cyber. Les assureurs bénéficieraient également de questionnaires plus pertinents permettant une évaluation plus fine du risque. L'objectif est de favoriser la convergence des questionnaires de sécurité utilisés par les assureurs, parfois déjà engagée par certains assureurs et évaluateurs. La réutilisation des réponses fournies en serait facilitée pour les TPE/PME. Dans un premier temps, cette option est plus aisée à mettre en place que des référentiels communs de sécurité dans la mesure où ces outils sont directement utilisés par les assureurs pour tarifer leurs contrats. Elle présente cependant comme limite de ne pas évaluer directement la robustesse de l'entreprise et nécessite aussi de définir un modèle de maturité cyber, décliné en questionnaires de sécurité.

Un groupe de travail, composé de représentants d'entreprises (MEDEF, CPME, CESIN, CLUSIF et AMRAE), de France Assureurs, de l'ANSSI, de la DGE et de la DGT pourrait notamment examiner à brève échéance ces deux solutions et travailler à leur mise en œuvre.

b) La mobilisation des réseaux de proximité, publics comme privés, permettrait de sensibiliser les TPE/PME au risque cyber

Afin de cibler de manière efficace le tissu économique local, il paraît justifié de mobiliser les acteurs de proximité pour sensibiliser au risque cyber. Sur le modèle du partenariat mis en place entre l'Agéa, France Assureurs et la gendarmerie nationale, les réseaux de distributions constituent l'échelon pertinent dans la mesure où ils ont une connaissance fine de leurs clients. Le maillage public, notamment les référents cybermenaces de la police nationale et de la gendarmerie nationale ou les organismes consulaires peuvent également jouer un rôle pour définir et mettre en place des actions de prévention au plus près du tissu économique local, notamment en mobilisant les ressources de cybermalveillance.gouv.fr. La mise en place de nouveaux partenariats entre les fédérations de professionnels, les organismes consulaires et les forces de sécurité est à envisager. Un groupe de travail dédié rassemblant ces acteurs pourrait travailler à la définition d'un plan de prévention cyber pour engager des actions de prévention dès 2023.

Le partenariat entre France Assureurs, l'Agéa et la gendarmerie nationale

En septembre 2021, France Assureurs a signé avec la Gendarmerie nationale et l'Agéa un partenariat inédit pour former et sensibiliser les agents généraux d'assurance au risque cyber. Cette coopération poursuit plusieurs objectifs :

- sensibiliser les agents généraux et leurs clients TPE/PME au risque cyber ;
- faciliter la coopération en matière cyber entre les agents généraux, les gendarmes et les experts en cyber sécurité, notamment à travers l'identification d'agents référents de la gendarmerie dans chaque département ;
- faire des agents généraux des acteurs de la prévention à travers des actions de formation dans les départements à destination des agents généraux et de représentants d'organisation professionnelle.

En 2021, trois conférences régionales sur la cybersécurité se sont tenues, réunissant en moyenne plus de 170 agents généraux. Sur le premier semestre 2022, sept actions de formations d'agents généraux ont été organisées au niveau départemental.

2.4.2. Le développement de l'offre de formation à la gestion du risque cyber pour les assurances et les réseaux de distribution est de nature à améliorer la qualité de l'accompagnement des entreprises

Il paraît pertinent d'agir sur la formation dans le secteur de l'assurance pour accompagner la montée en maturité des professionnels du secteur de l'assurance sur les enjeux de cybersécurité. L'ANSSI promeut déjà le développement de formations dans le domaine de la cybersécurité, notamment à travers le label SecNumEdu, décliné en SecNumEdu FC pour la formation continue.

Pour la formation initiale, il est envisageable de favoriser l'intégration de modules dédiés à la cybersécurité dans des cursus existants. Ces modules pourront s'appuyer sur les guides méthodologies développés par l'ANSSI. Surtout, un travail avec les responsables de formations spécialisées dans les métiers de l'assurance est nécessaire pour faire évoluer les maquettes pédagogiques et introduire des enseignements dédiés au risque cyber.

Enfin, il paraît nécessaire de développer l'offre de formation continue en matière de gestion des risques cyber. La diffusion par les fédérations de professionnels des formations généralistes des MOOC de l'ANSSI permettrait de pallier ce manque à court terme. À moyen terme, il paraît nécessaire d'engager un travail avec les instituts de formation professionnelle pour inclure des modules sur la gestion des risques cyber, en lien avec l'ANSSI et l'Institut des actuaires.

Un groupe de travail dédié, réunissant l'ANSSI, l'Institut des actuaires, les fédérations professionnelles ainsi que les principaux centres de formation continue et de l'enseignement supérieur pour les métiers de l'assurance, pourrait travailler à la mise en place de ces orientations.

2.4.3. Une *task force* de l'assurance du risque cyber, qui pourrait être adossée à Paris Europlace, permettrait de piloter la mise en œuvre des recommandations et faire de la place de paris un pôle d'expertise cyber

Le plan d'actions contenu dans le rapport constitue en soi une stratégie permettant l'affirmation de la place de Paris comme un pôle d'expertise cyber. La mise en place de ces actions nécessite un suivi et une gouvernance dédiés. En lien avec la direction générale du Trésor, une *task force* de l'assurance du risque cyber pourrait être chargée de piloter la mise en œuvre de la stratégie d'attractivité cyber. Elle devra mettre en place des synergies entre acteurs de la cybersécurité, les fédérations de professionnels, les entreprises ou encore les services de l'État et du régulateur.

Cette *task force* pourrait être composée de l'ANSSI, de l'ACPR, de l'AMRAE, de France Assureurs et de la DG Trésor. Elle pourrait également s'appuyer sur l'expertise de Paris Europlace et de Finance Innovation.

Annexes :

Tableau des recommandations

	Objectif	Mesure	Acteurs	Délai de mise en œuvre
Axe 1 : Clarifier le cadre juridique de l'assurance du risque cyber	Clarifier l'étendue des garanties cyber	Inviter les assureurs à adopter de bonnes pratiques de rédaction	ACPR	Court terme
		Élaborer un guide de place rappelant le cadre juridique et les bonnes pratiques	France Assureurs	Court terme
		Améliorer l'information de l'assuré sur les garanties cyber	État ou France Assureurs	Long terme
		Évaluer l'exposition des assureurs aux couvertures silencieuses	ACPR	Moyen terme
	Clarifier les clauses litigieuses	Conditionner l'assurabilité des cyber-rançons au dépôt de plainte de la victime	Mesure législative	Court terme
		Définir des modalités opérationnelles de coordination et de prévention des cyber-rançons	Ministère de l'intérieur, ministère de la justice, ANSSI, TRACFIN, DG Trésor, France Assureurs	Moyen terme
		Affirmer l'inassurabilité des sanctions administratives	Mesure législative	Moyen terme
		Approfondir les travaux sur l'exclusion de garantie pour cause de cyberguerre	DG Trésor, Ministère des armées, ANSSI, FA, AMRAE	Moyen terme
Axe 2 : Mieux appréhender et mesurer le risque cyber	Améliorer la prise en compte du risque cyber dans le pilotage de l'activité assurantielle	Favoriser la prise en compte du risque opérationnel cyber dans les ORSA	ACPR	Court terme
		Création d'une catégorie ministérielle et/ou une LOB dédiée et/ou une branche cyber	DG Trésor, ACPR, FA, partenaires européens	Moyen terme (Catégorie ministérielle) / Long terme (Branche)
	Répondre à la problématique de manque de données cyber	Mieux modéliser le risque et s'appuyer sur des méthodes innovantes de modélisation	Institut des actuaires, startups	Court terme
		Mise en place d'un Observatoire de la menace cyber	ANSSI, GIP Acyma, FA, DG Trésor	Moyen terme
Axe 3 : Améliorer le partage du risque entre assurés, assureurs et réassureurs	Renforcer la résilience des entreprises	Encourager le développement de captives de réassurance	DG Trésor	Court terme et effort à moyen terme
	Promouvoir des méthodes innovantes	Faciliter la constitution d'une offre d'assurance paramétrique	Institut des actuaires, l'ANSSI, Etalab, État, entreprises	Moyen terme
		Étudier le recours aux marchés financiers pour libérer de la capacité assurantielle	Task force cyber	Long terme
Axe 4 : Accroître les efforts de sensibilisation des entreprises au risque cyber	Encourager les PME à investir dans leur cybersécurité	Établir un modèle de cybersécurité déclinés en référentiels / harmonisation des questionnaires de sécurité	Représentants d'entreprises (notamment MEDEF, CPME et AMRAE), France Assureurs, ANSSI, DGE et DGT	Moyen terme
		Engager des actions de sensibilisation locale	Ministère de l'intérieur, ANSSI, fédérations professionnelles, chambres consulaires	Moyen terme
	Améliorer le capital humain	Formation initiale et continue des professionnels de l'assurance	ANSSI, l'institut des actuaires, les fédérations professionnelles, les principaux centres de formation continue et supérieur	Moyen terme

Membres du groupe de travail

Autorité de contrôle prudentiel et de résolution (ACPR)

Allianz Global Corporate & Specialty (AGCS)

American International Group (AIG)

Association pour le management des risques et des assurances de l'entreprise (AMRAE)

Agence nationale de la sécurité des systèmes d'Information (ANSSI)

AON

Association des professionnels de la réassurance en France (APREF)

Axa France

Axa XL

BESSE

Caisse centrale de réassurance (CCR)

CHUBB

CINOV IT

Consommation Logement Cadre de vie (CLCV)

COVEA

Confédération des petites et moyennes entreprises (CPME)

Direction générale du Trésor

DIOT-LSN

ENSAE Paris

France Assureurs

Generali

Groupement d'intérêt public action contre la cybermalveillance (GIP ACYMA)

Institut français des relations internationales (IFRI)

Institut des actuaires

MARSH

Mouvement des entreprises de France (MEDEF)

SIACI Saint Honoré

Société commerciale de réassurance (Scor)

Sorbonne Université

Swiss Re

Willis Towers Watson

Contributeurs extérieurs

Club des experts de la sécurité de l'information et du numérique (CESIN)

Citalid

Descartes Underwriting

Direction générale des entreprises

Direction générale de la gendarmerie nationale

Direction générale de la police nationale

Haut comité juridique de la Place financière de Paris

Hexatrust

Lloyd's

LSN

Taylor Wessing