LA MAÎTRISE DU RISQUE CYBER SUR L'ENSEMBLE DE LA CHAÎNE DE SA VALEUR ET SON TRANSFERT VERS L'ASSURANCE

Philippe Cotelle, Philippe Wolf, Bénédicte Suzan

▶ **To cite this version:**

Philippe Cotelle, Philippe Wolf, Bénédicte Suzan. LA MAÎTRISE DU RISQUE CYBER SUR L'ENSEMBLE DE LA CHAÎNE DE SA VALEUR ET SON TRANSFERT VERS L'ASSURANCE. [Rapport de recherche] 401, IRT SystemX. 2016. hal-02360152

HAL Id: hal-02360152
https://hal.science/hal-02360152v1

Submitted on 12 Nov 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

LA MAÎTRISE DU RISQUE CYBER SUR L'ENSEMBLE DE LA CHAÎNE DE SA VALEUR ET SON TRANSFERT VERS L'ASSURANCE

RÉSULTATS du Séminaire de RECHERCHE novembre 2015 - juillet 2016

EN PARTENARIAT AVEC

RAPPORT

ÉTABLI PAR

PHILIPPE COTELLE HEAD OF RISK MANAGMENT & INSURANCE AIRBUS DEFENCE AND SPACE	PHILIPPE WOLF PhD PROJECT MANAGER EIC IRT-SYSTEMX	BENEDICTE SUZAN PhD R&T AND INNOVATION COORDINATION (CIS) AIRBUS DEFENCE AND SPACE

POUR TOUT RENSEIGNEMENT CONCERNANT CE RAPPORT, VOUS POUVEZ CONTACTER L'IRT-SYSTEMX AUX COORDONNÉES CI-DESSOUS :

IRT SystemX
8, avenue de la Vauve
CS 90070 – 91127 Palaiseau Cedex
Site internet : www.irt-systemx.fr
Courriel : philippe.wolf@irt-systemx.fr

Droit de propriété intellectuelle

Cette publication est diffusée sur le site de l'IRT-SystemX, mais reste protégée par les lois en vigueur sur la propriété intellectuelle. Est autorisée la copie d'extraits de 500 caractères, suivis chacun de la mention « Source : » assortie de l'url de la publication SystemX. Toute autre reprise doit faire l'objet d'une autorisation préalable auprès de philippe.wolf@irt-systemx.fr

VERSIONS	Relecture	DATE	Modification
ISX-IC-EIC-transfert-risque-draft-v0	ISX et Airbus Group	17/06/2016	Version initiale
ISX-IC-EIC-transfert-risque-LIV-0401-v10	Groupe de travail	29/08/2016	Version diffusable

Table des matières

I. Présentation des travaux

Ce travail de recherche, mené au sein du programme EIC de l'IRT-SystemX[1], traite des **conditions nécessaires pour connaître, gérer et maitriser le risque cyber pour ensuite le transférer éventuellement vers l'assurance**. Le chapitre III résume les résultats obtenus. Les chapitres ultérieurs détaillent l'ensemble des réflexions menées. La grille de travail initiale, ci-dessous, a été suivie dans ses grandes lignes.

EIC T5.2 Cyber Assurance	Objet de la séance	Objectif de la séance	Résultats de la séance souhaitée	Livrable	Contributions
Première Année de la recherche (3 ans envisagés)	La première année sera consacrée à poser les problématiques. La réflexion portera sur la recherche des définitions partagée de l'exposition au risque cyber et de ses critères entre l'assuré et le client.				Le secrétariat des séances et la production écrite est assurée par EIC.
1er réunion 2h30 24 novembre	Présentation de la proposition de la recherche et de ses enjeux pour l'année et ses suites en fonction des résultats si ces derniers sont pertinents. Présentation du point de vue de l'assuré : de l'importance pour un industriel de monter en puissance dans la gestion de son risque cyber et son assesment et de sa capacité à dialoguer avec l'assurance et de confronter ses analyses de risque internes Présentation du point de vue de l'assureur : lever les blocages du marché de l'assurance. Présentation du point de vue de la puissance publique : les verrous à lever, les premiers axes d'action.	Présentation des travaux envisagés pour l'année. Exposer le besoin qu'ont les organisations de maîtriser la gestion de leur risque cyber dans un dialogue avec les assureurs. Expression des besoins des assureurs-ré assureurs. Montrer comment le législateur peut aider.	Recherche d'un Accord sur : L'utilité de mener un dialogue tripartite entre industriels, assureurs-réassureurs et les pouvoirs publics et/ou associations professionnelles. Les points de blocages, les définitions et les objectifs de la réflexion à mener. Accord sur les principes de la méthode et les apports et attendus de chacun des participants. Accord sur la finalité de la recherche.	Compte rendu de séance. Document comprenant une taxonomie, l'identification des verrous techniques et règlementaires. Road map, calendrier des activités et des apports des parties prenantes.	Appel à contribution auprès des partenaires. Mise à disposition des ressources juridiques d'EIC à l'appui de T5.2.

[1] **EIC : Environnement pour l'Interopérabilité et l'Intégration en Cybersécurité**. Les annexes 1, 4 et 5 détaillent le contexte de réalisation de cette étude

2e réunion 2h30	Statistiques de marché : les assureurs manquent de données et de modèles d'anonymisation agréés et utilisables par tous.	Produire une définition et une qualification de l'incident cyber du point de vue de l'assuré et de l'assureur. Proposer des critères communs et factuels montrant qu'une organisation répond aux exigences de protection face au risque cyber.	Définir les conditions d'un accord-cadre de référence interne (pour les organisations) et externe (pour les assureurs et réassureurs).	Compte rendu de séance. Rapport de de synthèse illustrant les problématiques et le consensus obtenu exposant les avancées de la réflexion. Document décrivant les moyens d'établir des modélisations.	
3e réunion 2h30	Couverture : quel est le besoin de couverture de l'assuré pour le risque cyber ?	Adresser la question du recouvrement de la perte de propriété intellectuelle, de la R&D et de la perte de données d'exploitation ou de moyens de production. Comment gérer l'évènement catastrophe (le scénario d'accumulation), quelles sont les responsabilités du client, de l'assureur et de la puissance publique ? L'enjeu d'une méthodologie pour calculer les sinistres maximum possibles, une mutualisation est-elle envisageable ?	Produire les premiers éléments	Compte rendu de session. Document synthétique illustrant les problématiques et le consensus obtenu exposant les avancées de la réflexion.	
4e réunion 2h30	Information de souscription et de gestion du risque cyber : nécessité d'un représentant assermenté.	Discuter la proposition suivante : en l'absence actuelle de statistiques de marché et au vu des couvertures existantes, comment créer les conditions générales d'un dialogue de confiance entre le client et l'assureur ? Quel rôle pour la puissance publique ?	Définir les conditions d'un dialogue de confiance entre l'assuré et l'assureur. Définir le tiers de confiance qui permettrait la collecte, la validation et l'anonymisation des données permettant la construction des modèles Proposer la création d'un organisme paritaire définissant le contenu et la validation d'une formation qualifiante d'Experts Cybers Assurance	Compte rendu de session. Document synthétique illustrant les problématiques et le consensus obtenu exposant les avancées de la réflexion.	

5e réunion conclusive 2h30	**Présentation des travaux réalisés sur l'année, proposition de document conclusif.**	**Consolidation du cadre de référence, des critères communs et de la méthodologie.**	**Accord sur les standards Et sur la diffusion des résultats de la recherche. Proposition d'un plan d'action.**	**Présentation du rapport conclusif sur les trois pistes de travail proposées lors de la première séance.** **Rapport de recherche présentant une proposition de critères communs et un standard.** **Présentation du plan d'action devant conduire à la mise en œuvre des critères communs et des standards, concevoir leur contrôle.** **Présentation des moyens nécessaires pour ce faire.** **Proposition - En fonction des opportunités : Publication des résultats de la recherche. Organisation d'un colloque d'une demie-journée avec le soutien de l'ANSSI.**	

Figure 1 – Plan de travail

II. Méthode suivie

Ce travail de recherche a été mené par une équipe pluridisciplinaire regroupant assureurs, réassureurs, courtiers, associations professionnelles, juristes, un *risk manager*, des industriels, une organisation internationale, des organismes publics et des chercheurs. Les annexes 2 et 3 listent les participants à ces travaux.

Des **séminaires réguliers** ont confronté les points de vue et les réflexions sur les diverses thématiques de la figure 1. Un consensus a été obtenu autour des **cinq recommandations consolidées** du chapitre III.3. Les chapitres IV à VII détaillent la variété des approches et des pistes explorées qui doivent être approfondies dans des travaux ultérieurs décrits au chapitre III.4.

La réunion 1 – introductive (novembre 2015). L'objet de cette réunion était, outre la présentation du projet de séminaire et de la proposition de recherche, de poser l'interrogation du *risk manager* quant à la prise en compte et la gestion du risque numérique (cyber) : comment penser un cadre normatif pour prendre en compte le risque numérique ? Quelle trame proposer ?

Airbus Group a présenté son retour d'expérience sur l'exercice SPICE – *Scenario Planning for Indentification of Cyber Exposure* – développé en interne en 2015. SPICE permet d'affecter une valeur financière à l'exposition au risque numérique d'une ampleur catastrophique pour la pérennité d'une organisation. Cette démarche utilise des informations recueillies auprès des opérationnels pour quantifier l'impact métier d'une attaque majeure et établir des scenarii. Exercice reconductible annuellement, il permet au *risk manager* d'identifier, de gérer et de maîtriser son exposition au risque et d'engager un dialogue avec le marché pour son transfert vers l'assurance. Il a été proposé de faire de la démarche SPICE un standard pour l'évaluation de l'exposition au risque numérique et de ne pas utiliser de scénario standard mais une analyse de risque propre à chaque organisation qui prenne en compte le risque numérique dans le métier.

La réunion 2 – Catégories communes, définition, qualification et quantification (janvier 2016) – a présenté un tableau des causes et des conséquences. Les travaux préparatoires de la réunion 2 ont constitué un premier effort de définition de métriques, de faits dommageables et de conséquences préjudiciables sur l'exemple du tableau de Mendeleïev. L'objectif étant de produire des « briques » pour constituer les scenarii d'exposition au risque numérique : une suite d'évènements / d'éléments prédéfinis auxquels sont associées des métriques objectives. Leur complexité combinatoire comme celles des molécules, des atomes et leurs combinaisons constituant le scenario complexe de l'attaque cyber. L'objectif est de proposer un système logique cohérent pour illustrer les scenarii d'attaque cyber. Les définitions des métriques, des faits dommageables et des conséquences préjudiciables ont été préparés avec les juristes.

Un *reality check* a été ensuite organisé (en mars 2016) pour tester si le tableau des causes et des conséquences fonctionnait. Il a montré que l'exercice du tableau permettait, en effet, de jouer des scenarii d'attaque cyber. Ceux qui ont été joués étaient des cas réels avérés rendus publics ou récupérés par les acteurs du marché. La matrice a néanmoins fait l'objet d'un travail de récriture en séance.

La réunion 3 – Couverture et gestion des scenarii par les assurances (avril 2016). Cette réunion avait pour objectif de montrer comment le marché pourrait répondre à l'ensemble des cas de causalité et de conséquences et par quelles couvertures assurantielles il pouvait être envisagé de couvrir le risque numérique. Le tableau *mapping* des couvertures assurance a été réalisé à partir du tableau des causes et conséquence et surtout à partir des travaux déjà réalisés par les assureurs au sein de la FFSA (Fédération Française des Sociétés d'Assurance devenue FFA en juillet 2016). Un document novateur et unique.

La réunion 4 – Information de souscription (mai 2016) porte sur les conditions qui permettront le dialogue entre assurés et assureurs. Comment construire le dialogue (ses conditions), comment les parties prenantes pourraient communiquer sur les informations de souscription, comment gérer la confidentialité, comment organiser la déclaration des sinistres et comment répondre à la question de la quantification de la perte (le recours à des experts).

Une réunion supplémentaire a été consacrée à la présentation des premiers résultats de la recherche et ses propositions de recommandation.

La réunion 5 – Réunion conclusive. Elle est dédiée à la présentation pour adoption du rapport de recherche et aux décisions pour la suite des actions et travaux.

De nombreuses réunions ont été organisées en parallèle par Philippe Cotelle et/ou Bénédicte Suzan pour avancer sur différents points.

III. Résumé des résultats obtenus

III.1. Constat

De plus en plus conscientes de la menace que le risque cyber fait peser sur leur activité, les entreprises et autres organisations s'efforcent de quantifier leur exposition au risque cyber toujours plus précisément. Elles se heurtent toutefois à de nombreux obstacles dans la connaissance, l'appréhension et la gestion de ce risque. En l'absence de procédures fiables pour soutenir leur démarche, les gestionnaires de risques n'ont souvent pas encore développé une approche globale du risque cyber sur l'ensemble de la chaine de valeur, ni intégré sa dimension potentiellement catastrophique pour la pérennité de l'activité de l'entreprise. Nombre d'entre eux s'interrogent sur l'opportunité d'investir dans des couvertures assurantielles cyber, en prenant conscience que la sécurisation de leurs systèmes d'information et la protection de leurs infrastructures, leurs produits et leurs données stratégiques ne les mettront jamais à l'abri de toutes les attaques.

Les données chiffrées publiques et privées sur le coût des cyber-attaques sont, à ce stade, insuffisantes : on ne dispose ni de suites statistiques sur une durée suffisamment longue, ni de métriques largement validées pour définir le coût global des attaques passées ou pour établir des modèles économiques fiables permettant de prévoir les préjudices liés aux futures attaques informatiques.

Ces obstacles brident le développement du marché de la cyber-assurance. Si toutes les parties prenantes s'accordent sur son fort potentiel, ce marché, qui s'est d'abord développé aux Etats-Unis, demeure embryonnaire, notamment en Europe.

Parallèlement, les pouvoirs publics nationaux et internationaux se sont également saisis de la question de la gestion des cyber-risques et de leur éventuel transfert en vue de renforcer la résilience des acteurs économiques. Dans certains pays, des outils réglementaires ou législatifs ont été développés.

Le cyberespace est définitivement différent du monde réel car il obéit à des lois d'une autre nature : les réseaux numériques n'ont pas de frontières, sont extensibles à l'infini et sont de nature abstraite et virtuelle ; le temps et l'espace y sont comprimés ; les attaquants potentiels sont parfois vos proches voisins ; les transitions y sont indécelables ; les précurseurs d'une attaque sont des événements très difficiles à percevoir ; les identités sont difficiles à discerner et les actions y sont ambigües. Le caractère malveillant d'un code informatique n'est pas une caractéristique intrinsèquement prouvable.

Enfin l'économie numérique défie l'économie traditionnelle : le coût d'une attaque peut être marginal (gratuité des outils) par rapport au montant des conséquences ou au coût de protection des Systèmes d'Information.

Le risque numérique est aujourd'hui mal appréhendé :

- La numérisation de l'ensemble des activités humaines depuis l'entreprise jusqu'au domicile augmente les surfaces d'attaque et rend nécessaire une prise en compte du risque numérique dans l'ensemble des strates de la société ;
- Il est aujourd'hui difficile d'avoir des références et un vocabulaire commun car la menace évolue sans cesse même si les fondamentaux restent les mêmes ;
- Le manque de données chiffrées publiques et privées concernant le coût des attaques dont les méthodes de calcul seraient validées par l'ensemble de la communauté et l'absence de recul statistique et de modèles économétriques rend difficile l'évaluation des préjudices liés aux attaques informatiques ;
- Pour une organisation, la quantification du risque cyber, à savoir le calcul de l'impact économique et financier d'un aléa cyber sur sa chaine de valeur est désormais incontournable. Cette valorisation lui permettra de répondre à la question de son transfert à l'assurance ;
- Les méthodologies assurantielles ne sont pas encore assez consolidées/établies pour chiffrer le risque cyber. Il n'existe pas aujourd'hui de **métrique éprouvée** permettant d'évaluer de manière précise le coût d'une attaque cyber et de déterminer des stratégies de réduction et de transfert par l'assureur. L'état de l'art est encore peu mature sur ces questions.

Néanmoins, le ***risk manager*** **prend la mesure de l'importance du risque cyber et de sa nécessaire maîtrise dans un dialogue constructif avec le monde de l'assurance**. Il se heurte à de nombreux obstacles dans la connaissance, l'appréhension et la gestion de son risque en interne et il ne dispose pas encore de **référentiels, critères et standards** pour soutenir sa démarche. Les référentiels du management du risque des entreprises n'ont pas encore développé une approche compréhensive et intégrée du risque cyber sur l'ensemble de la chaine de sa valeur et également dans une dimension catastrophique pour la pérennité de l'activité de l'entreprise. Le *risk manager* doit s'approprier le risque cyber et ne plus le laisser aux fonctions informatiques de l'organisation et aux techniciens de la cyber sécurité.

Le projet de recherche s'efforce de répondre aux besoins du *risk manager* pour l'aider dans sa maîtrise du risque cyber et le transfert, le cas échéant, de tout ou partie de celui-ci au marché de l'assurance.

La première année du projet a porté sur les causes et les conséquences des incidents cybers ainsi que sur les différentes lignes d'assurance qui permettent de les couvrir. Les travaux ont tenté de mieux définir également les informations nécessaires à la souscription. Une réflexion a été menée autour de la création d'un organisme paritaire définissant le contenu et la validation d'une formation qualifiante d'experts Cyber Assurance. Ces derniers seraient les tiers de confiance qui assisteraient les entreprises et organisations dans la quantification de leur risque cyber et permettraient en outre la collecte, la validation et l'anonymisation des données nécessaires à la construction de modèles permettant de modéliser les risques cyber.

Ces travaux constituent un socle de référentiels que les assurés, les assureurs et réassureurs pourraient être invités à partager.

III.2. Objectifs de la recherche

Les travaux de recherche appliquée portent sur les conditions nécessaires pour connaître, gérer et maitriser le risque cyber ainsi que pour le transférer au marché de l'assurance lorsque cela est jugé opportun.

Plus particulièrement, l'objectif du groupe de travail est d'identifier les obstacles à la compréhension et l'évaluation du risque cyber et ceux qui entravent notamment le développement du marché de l'assurance cyber. Il s'est également agi d'avancer sur certains points et de produire des premières recommandations. Un *White Paper*, rédigé sur la base de ce rapport de recherche, proposera ensuite un plan d'action en fonction des calendriers législatifs et réglementaires en cours (nationaux et internationaux).

Les organisations privées et publiques commencent à s'interroger sur la définition de leur exposition. Mais elles peinent à exprimer leurs besoins, à comprendre leurs expositions au risque et à s'en protéger efficacement. D'autant que le coût tant des couvertures assurantielles cyber que des investissements nécessaires à la sécurisation de leurs systèmes d'information et à la protection de leurs infrastructures, leurs produits et leurs données stratégiques est élevé. Elles s'interrogent quant au transfert vers l'assurance de tout ou partie du risque cyber qui, de plus, peut déjà être couvert par d'autres garanties de contrat déjà souscrits.

Les pouvoirs publics nationaux et internationaux se saisissent également de la question et s'interrogent sur les moyens à mettre en œuvre pour favoriser et créer les conditions d'un dialogue constructif et élaborer les outils réglementaires ou législatifs nécessaires.

Les réflexions de ce groupe de travail portent attention à la problématique de la réassurance car le cyber-risque est considéré comme un risque systémique. La crainte de ses effets systémiques (impacts sur des chaînes de sous-traitance, atteintes à la réputation, atteintes à la société civile, dommages en cascade non anticipés et maîtrisés, etc.), la rapidité d'évolution des technologies et la fréquence du renouvellement des scénarii d'attaque le font considérer comme le risque futur le plus important (territoires intelligents, robotisation croissante, transport intelligent, exploitation des données personnelles).

La première année, les travaux ont porté sur la définition de l'exposition au risque cyber. Ils ont conduit à proposer

- des catégories communes, des définitions partagées, une qualification et une quantification de l'incident cyber ;
- des lignes d'assurance qui permettent de les couvrir ;
- de progresser sur l'information de souscription : les conditions de la confidentialité.

Les travaux et la démarche d'analyse de risque de l'exposition au risque cyber qui constitue le socle de la réflexion du séminaire s'est inspirée des travaux de référence NIST (*National Institute of Standard and Technology – USA*) et de l'ENISA (l'Agence européenne de la sécurité des Systèmes d'information. La rédaction de la LPM (Loi de Programmation militaire) – OIV (Opérateur d'importance vitale) s'inscrit dans la ligne de la loi européenne (NIS directive – *Network and*

Information Security) et est alignée avec les travaux du GGE (Groupe d'experts gouvernementaux) de l'ONU.

Les travaux s'inscrivent dans une démarche internationale.

III.3. Recommandations consolidées

Recommandation 1

Chaque entreprise devrait **conduire une analyse financière du risque cyber pour :**

- analyser ses **impacts opérationnels** ;
- définir le **niveau adéquat d'investissement** pour sa prévention et protection ;
- en déduire les **risques transférables à l'assurance**.

Cette analyse doit être orchestrée par le ***risk manager***[2] qui doit faire l'interface entre les impératifs opérationnels des fonctions et les contraintes de sécurité que rencontre son organisation. Cette analyse de risque cyber doit s'appuyer sur des scénarii critiques établis avec les opérationnels. Elle doit consister en l'identification de scenarii catastrophiques pour la conduite des affaires et une quantification financière des conséquences de ces scénarii et de leur développement dans le temps. Cet exercice permettra de dimensionner l'exposition à ce risque ainsi qu'une meilleure prise de décision sur des politiques de réduction de risque.

La présentation de la démarche du pilote *Airbus Defence and Space* SPICE a permis d'éclairer de façon concrète comment ce processus peut être mis en place.

Le chapitre IV développe cette recommandation.

Recommandation 2

Il est utile de définir un **référentiel et un langage commun** permettant de mener les analyses de risque cyber en vue de leur transfert vers l'assurance. Ce référentiel commun va permettre de définir un cadre utile pour référencer puis comparer relativement les expositions au risque de différentes entités. **Nous recommandons que leurs propres scénarii d'exposition soient décomposés selon les catégories de risques élémentaires** (combinaison de fait générateurs et de conséquences) qui représentent un cadre d'analyse commun à l'ensemble des entités quel que soient leur taille, nature et activité.

Les travaux de recherche font une proposition novatrice d'un cadre référentiel d'analyse de risque cyber avec des catégories élémentaires qui ambitionnent de répondre, par leur association, à

[2] Il faut également approfondir cette démarche pour répondre aux enjeux des TPE – TPME dans la définition de leur exposition au risque cyber et son transfert vers l'assurance. Dans la suite du texte nous parlerons du *risk manager* comme d'une fonction générique couvrant également les professionnels venant en appui des organisations dont la taille ne permet pas la création d'un poste dédié.

l'ensemble des scénarii pouvant affecter les entités. Ces concepts permettent aux entités qui le souhaitent de bâtir leur propre référentiel (respect du droit de la concurrence).

Ce cadre d'analyse commun représente une avancée considérable dans la rationalisation des mesures de risques et dans la possibilité de mapper relativement le profil de risque des différentes entités dans un référentiel partagé.

Le chapitre V développe cette recommandation.

Recommandation 3

Une meilleure communication et connaissance des couvertures d'assurance couvrant les conséquences du risque cyber doit être développée. Les *risk managers* et porteurs de risques ont besoin de mieux comprendre la façon dont les différentes couvertures protégeant leurs entités se combinent pour répondre à cette exposition. La **matrice** développée dans le cadre de ce programme de recherche est un outil permettant :

- aux *risk managers* de pouvoir vérifier comment les différentes couvertures souscrites permettent une couverture effective et globale des besoins de leurs entités ;
- à l'ensemble des parties prenantes de mieux comprendre les couvertures d'assurance en clarifiant les garanties qui relèvent de polices d'assurance traditionnelles de celles relevant de polices cyber dédiées. La présence de couvertures silencieuses (*silent cover* ou, autrement dit, lorsque le risque cyber n'est pas expressément exclu) peut ainsi être plus facilement identifiée ;
- aux autorités nationales de disposer d'une photographie instantanée de la réponse de leur marché d'assurance à ce risque ;
- aux organisations internationales de disposer d'une meilleure vision du sujet. Cette matrice peut effectivement devenir également le support à un benchmark international en comparant la réponse des différents marchés nationaux à cette même exposition.

Cette matrice pourra être exploitée par l'ensemble des acteurs, sans exclusive ni obligation, notamment dans le cadre de benchmarks internationaux. Elle pourra être simplifiée pour être plus facilement utilisable par de petites entités.

Le chapitre VI développe cette recommandation.

Recommandation 4

Concernant **la gestion de la confidentialité dans le dialogue** pour l'information de souscription et la gestion du sinistre, la mise en place d'une plateforme neutre et sécurisée de communication et d'échange d'information entre les assurés et les assureurs est indispensable pour améliorer le dialogue. Un meilleur dialogue permettra aux assurés de donner une meilleure visibilité sur leur exposition et gestion du risque cyber pour une meilleure adéquation de la souscription par les assureurs des couvertures souhaitées. Elle permettra un meilleur échange en cas de sinistre dans le cadre d'une relation dont la confidentialité sera garantie.

Trois types de structure peuvent être envisagés :

- une extension, dont les contours juridiques restent à définir, de la « plateforme d'assistance aux victimes de cyber malveillance », mise en place par l'ANSSI avec le ministère de l'Intérieur (annoncée dans la Stratégie Nationale pour la sécurité numérique[3] présentée le 16 octobre 2015) ;
- une autre plateforme neutre d'échange d'information entre l'assureur et l'assuré. Elle serait opérée par un tiers de confiance. Cette « Plateforme mutualiste sécurisée pour la maîtrise et l'assurance du risque cyber » serait à but non commercial. Sa forme juridique reste à définir.
- un « observatoire national de risque cyber ». Un modèle possible est l'Observatoire National des Risques Naturels[4]. Cette structure pourrait permettre par un processus d'anonymisation, la mise en place de statistiques fiables qui aideront la meilleure quantification d'une tarification adaptée du risque. Il s'agirait également de réfléchir à la qualification de l'expert tiers de confiance.

Le chapitre VII développe cette recommandation.

Recommandation 5

Un travail de normalisation du dialogue doit être engagé. Il s'agit de poursuivre l'exercice de convergence des vocabulaires techniques, assurantiels et juridiques.

En particulier pour atténuer le recours au contentieux, il s'agit de créer le continuum et la convergence entre les éléments techniques, assurantiels et juridiques pour définir le périmètre du contrat, les champs de responsabilité et leurs limites.

Il faut, pour cela, conduire un exercice de compilation des définitions contractuelles et réglementaires et proposer des définitions, probablement médianes (sur le modèle du PPP Britannique *Cambridge University*), adaptées à la dimension internationale des entreprises.

Il est également nécessaire :

- d'identifier les lacunes du droit du numérique pour renforcer la sécurité juridique dans les contrats d'assurance ;
- de suivre l'évolution de droits différents (Common Law) ;
- de créer la qualification juridique de la donnée immatérielle, l'identification des atteintes qu'elle peut subir afin de permettre la quantification de sa valeur.

Il peut s'avérer pertinent d'associer à cette réflexion les professions des experts comptables, des commissaires aux comptes et de la finance d'entreprise.

Le chapitre V développe cette recommandation. L'Annexe 7 fournit les premiers éléments pour l'élaboration de définitions communes.

[3] http://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf
[4] Voir http://www.onrn.fr/

III.4. Travaux ultérieurs

L'ensemble de ces 5 recommandations définit des points à travailler collectivement pour progresser dans la compréhension et la maitrise du risque cyber.

I. Bâtir un langage commun : De quoi parle-t-on ?

a) Techniquement :

Définir les risques informatiques liés au cyber dans un langage français et compréhensible par tous

b) Juridiquement :

Qualifier juridiquement la donnée informatique

Conduire un exercice de compilation des définitions contractuelles et réglementaires, proposer des définitions médianes, en s'inspirant éventuellement du modèle du PPP Britannique Cambridge University

II. Identifier les éventuels risques juridiques

Analyser les conséquences de ces nouveaux risques sur l'environnement juridique (règlementaires, législatifs..)

Identifier les nouvelles zones d'incertitudes juridiques et proposer des évolutions du droit afin de sécuriser les relations contractuelles entre assurés et assureurs exemple : Assurabilité des rançons, amendes pénales etc…

III. Travailler sur les métriques

Une connaissance statistique des enjeux est un préalable à tout transfert à l'assurance.

Cette connaissance passe par une maitrise de l'exposition et de l'aléa.

a) L'exposition : Quantifier le cout du risque cyber

Poursuivre la réflexion sur la quantification du risque cyber (avec le concours des travaux de recherche entamés à l'IRT).

Développer la recherche pour la quantification du risque cyber au sein des entreprises, notamment en tenant compte des conséquences induites par la nouvelle règlementation européenne GDPR. Aider les entreprises, les conseils et les assureurs à mieux répondre à la question : comment évaluer le cout du risque pour les entreprises ?

b) L'aléa : Bâtir une Base de données des événements cyber

Les événements cyber doivent être référencés, regroupés par nature et évalués au sein d'une base de données.

Inclure dans la réflexion les actuaires, les *Chief Data Officers* et les *Digital Officers*.

Proposer un modèle de remontées des données via les différentes sources disponibles (assureurs, pouvoirs publics, autres …) afin de pouvoir en extraire des statistiques fiables et partagées.

IV. Transfert des cyber risques à l'assurance

a) Partager une définition commune du périmètre d'intervention de l'assurance

Valider, Valoriser et Communiquer sur la matrice des risques et leurs définitions proposées dans le cadre de ce GT afin de faire émerger un référentiel crédible, reconnu et partagé. Cela pourra permettre d'améliorer la compréhension et la confiance des différentes parties prenantes, voire d'aider à la convergence des pratiques des différents intervenants pour améliorer la qualité et l'adéquation des offres.

b) La couverture du risque terroriste cyber.

Analyser les conséquences d'une cyber attaque à des fins de terrorisme, valider la capacité du marché de l'assurance à intervenir dans ce cas et étudier, si besoin, des solutions alternatives comme le GAREAT en a bâties pour le risque terrorisme matériel.

V. Créer la confiance

a) Une culture du risque à faire progresser

Encourager, promouvoir les actions à destination du grand public et des entreprises pour améliorer la connaissance du cyber risque.

b) Développer des référentiels

Donner les moyens aux entreprises de qualifier facilement le professionnalisme des différents intervenants à la maîtrise à la réduction et au transfert du risque cyber (notamment conseils, audit, prévention, protection, instruments financiers, assurance…)

c) Développer les conditions de la confidentialité :

Quel rôle de la puissance publique :

En complément de la plateforme annoncée de l'ANSSI, étudier l'opportunité de mettre en place une plateforme neutre d'échange d'information entre l'assureur et l'assuré. Elle pourrait alors être opérée par un tiers de confiance à définir. Cette « Plateforme mutualiste sécurisée pour la maîtrise et l'assurance du risque cyber » pourrait être à but non commercial sous la forme d'un Partenariat Public-Privé entre une « émanation » de l'ANSSI et des entreprises d'assurance. Sa forme juridique serait à définir.

S'assurer de la confidentialité du dialogue entre assureurs et assurés

Tant au niveau de la souscription et de l'indemnisation, développer un climat de confiance et de confidentialité permettant aux assurés d'informer en toute transparence et de manière exhaustive leurs assureurs pour réaliser le transfert de leur risque de manière optimale et être indemnisé dans les meilleurs conditions.

Pour cela engager une réflexion pour les TPE et PME d'un côté et pour les grands groupes de l'autre concernant la nature, le niveau nécessaire et les garanties d'informations de souscriptions dont a besoin le marché tout en respectant la liberté contractuelle de chaque assureur à définir lui-même les informations dont il a besoin pour tarifer et assurer les risques.

IV. La Connaissance du Risque Cyber par le *Risk Manager*

Verrous à lever

Méconnaissance voire absence de méthode et de standard pour définir l'exposition financière au risque cyber pour une organisation du point de vue de son transfert vers l'assurance.

Le *risk manager* a besoin de connaître son exposition au risque.

Le *risk manager* a besoin de dialoguer avec le marché.

Pour un dialogue constructif, les parties doivent partager une connaissance commune des sujets.

IV.1. Une démarche novatrice pour que le *risk manager* détermine son exposition au risque cyber

Le *risk manager* dispose d'outils pour apprécier les différents risques auxquels est confrontée son organisation. Dans une grande entreprise (ex. *Airbus Defence and Space*)[5], une activité « top down » offre une photographie annuelle de l'ensemble des paramètres des risques inhérents à chaque entité du groupe à qui sont adressés quelques 150 « Risk questionnaires ». Une fois consolidées, ces informations constituent la base d'un outil *corporate* qui a pour vocation de donner une vision précise et détaillée de l'exposition macroscopique. Cet outil est ensuite transmis aux assureurs du Groupe dans le cadre de la souscription des polices. Cette démarche « top down » constitue un processus d'amélioration continu.

Le *risk manager* détermine les risques sur lesquels il y a une criticité sur la cartographie en collaboration avec les responsables commerciaux et chefs de projets afin d'apporter des solutions assurantielles adaptées. Dans la mesure où Airbus Group reçoit environ une vingtaine de propositions commerciales de rang 1 par mois (+ de 100 millions d'euros), les cartographies doivent être dynamiques et rapides. Elles sont ensuite évaluées en « *Risk Management Committee* », revue formelle organisée pour l'ensemble des propositions assurantielles.

Concernant le risque cyber, il n'existe pas de photographie annuelle de l'ensemble de ses paramètres ni de cartographie maîtrisée des risques, or il incombe à sa fonction, dans le cadre de sa politique d'assurance des risques, de décider quels sont les risques numériques que souhaite assurer son organisation, à quel prix et avec quelle méthode afin d'établir son portefeuille d'assurance.

Or, l'état de l'art montre que ce risque n'est pas encore pris en compte comme le sont les autres risques d'entreprise. Il n'existe pas de méthode consolidée ni de standard partagé. Le *risk manager* doit être créatif pour répondre et interagir avec ses interlocuteurs habituels. Il doit être en mesure de répondre à la question posée simplement : quelle est le niveau d'exposition au risque cyber auquel l'organisation est confrontée afin d'étudier les conditions d'une partie de son transfert vers le marché de l'assurance.

[5] Philippe Cotelle, *Les 1001 facettes du Risk Manager*, Atout Risk Manager, La Revue des Professionnels du Risque et de l'Assurance, n°9, Juin 2016.

Pour répondre à cette question, *Airbus Defence and Space* a développé, avec l'appui de l'entité *CyberSecurity*, dont la mission consiste à proposer des solutions pour maîtriser le risque cyber technique pour le Groupe et pour ses clients, une démarche novatrice.

Sur la base de l'expertise technique d'*Airbus Defence and Space —CyberSecurity*, le *risk manager* de l'entreprise a développé une méthode innovante qui produit une analyse quantifiée de l'impact business et financier lié au risque cyber au travers du pilote SPICE – *Scenario Planning for Identification of Cyber Exposure* – développée en interne au printemps 2015.

Cette analyse est innovante par rapport aux analyses plus traditionnelles.

Les analyses de risque cyber de type MARION[6], MEHARI[7], EBIOS[8] (mécanique de conformité, conforme au modèle idéal), IS027005[9] qui traitent du risque cyber technique ne permettent pas de qualifier et de quantifier le risque cyber dans une logique assurantielle (financière).

De plus, ces méthodes portent sur des mesures IT et s'appliquent volontiers dans des environnements de sécurité périmétriques : un système d'information (SI) central et protégé comme un château fort (système protégé). On savait qui se connectait à quoi et qui faisait quoi. Etaient assurés le *hardware*, le *software* et les sauvegardes. Or, aujourd'hui le SI des grands groupes comme celui des PME s'étend bien au-delà de l'entreprise : le cloud etc… Les données sont sorties du château fort. Elles sont aussi chez le prestataire, le client, dans des clefs USB, dans le cyberespace…

Ces méthodes ne permettent pas de comprendre l'impact business d'un incident cyber et a fortiori celui d'un scénario catastrophe cyber. Elles ne permettent pas de formuler une quantification financière du risque cyber. En effet, une quantification financière accrochée à un modèle mathématique de présomption de menaces (en mode déterministe à défaut de disposer d'un mode probabiliste) afin de mettre en corrélation les mesures de sécurité présentes ou absentes et les présomptions de menaces en découlant, présomptions susceptibles de faire l'objet d'une garantie, ne fonctionne pas.

Le pilote SPICE a permis de franchir la distance qui sépare les méthodes d'analyse de risque IT et le besoin d'analyse du risque cyber du point de vue du *risk manager* dans une démarche assurantielle. Il permet de répondre à la question : quel est le risque cyber auquel est exposé une organisation au regard de son activité et au regard de son niveau de numérisation (une organisation est d'autant plus exposée qu'elle est très informatisée) ?

Ainsi, dans la mesure où le risque numérique est lié à l'activité propre de l'entreprise et en considérant le manque de recul historique et statistique, il nous paraît inutile de réfléchir en termes de bibliothèque de scénarios catastrophe cyber par domaine d'opération ou par secteur d'activité. Il

---

[6] Cette méthode déterministe a abandonné l'axe probabilité et a mis en corrélation des présomptions de menace par rapport à des techniques de sécurité présentes ou absentes : un système équilibré, cela ressemble à ça.

[7] MEHARI 2010 : https://www.clusif.asso.fr/fr/production/mehari/download.asp

[8] EBIOS 2010 : http://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/

[9] Voir https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory

faut partir de la connaissance métier des opérationnels qui appréhendent la sensibilité de leurs biens essentiels ou *assets*. Ces derniers sont actuellement les plus à même d'identifier le risque numérique majeur auquel les *assets* qu'ils manipulent sont exposés. Il n'existe donc pas de scénario de risque numérique standard et homogène utilisable par toutes les sociétés.

La proposition de recherche de ce séminaire pour traiter la maîtrise du risque cyber sur la chaîne de sa valeur et son transfert vers l'assurance s'appuie sur la démarche du pilote SPICE.

Le *risk manager* conduit d'abord en interne un exercice de ce type. Une fois qu'il connait son niveau de risque, son niveau d'exposition, après qu'il ait apporté des éléments financiers chiffrés qui permettent aux dirigeants de l'organisation de statuer sur les efforts d'investissement à conduire pour élever le niveau de protection cyber, il demeure un risque résiduel qui nécessiterait un niveau d'investissement trop important et qu'il est alors préférable de transférer au marché.

Le marché de l'assurance n'est pas le seul marché, par principe, en mesure d'absorber ce risque. Comme le montre la prise en charge des nouveaux risques (à grande échelle ou technologiques), les organisations peuvent préférer se tourner vers l'auto-assurance (*self financing*), les risques syndiqués par plusieurs entreprises d'assurance (*pools*, etc.) et/ou le transfert des risques aux marchés financiers.

La situation dans laquelle se trouvent les entreprises industrielles multinationales est d'être exposées par leur taille et la nature de leurs activités à des risques élevés que les assureurs hésitent à couvrir, ou, a contrario, les grandes entreprises peuvent renoncer à payer des primes élevées pour s'assurer estimant que le capital pourrait être mieux investi.

Néanmoins, ces organisations se doivent de réfléchir en termes de transfert du risque vers l'assurance car concernant le risque cyber, un scenario catastrophe cyber pourrait mettre en danger la pérennité de leur *business*, leur existence et entrainer leur faillite. Elles doivent également prendre en compte leur Responsabilités civiles professionnelles mais également la Responsabilité civile de leurs mandataires sociaux.

En séance de travail, la présentation de la démarche du pilote SPICE a soulevé les questions suivantes :

- Quels sont les différents impacts à prendre en compte ?
- Quels sont les métriques à utiliser ?
- Quels sont les éléments financiers, temporels et techniques à prendre en compte ?
- Est-ce que les conclusions d'une méthodologie similaire à SPICE répondent aux enjeux de souscription ?
- Est-ce qu'un assureur peut exploiter les résultats de SPICE pour souscrire ?
- Quels sont les avantages/inconvénients par rapport aux questionnaires de souscription qui sont à la fois plus statiques et plus techniques ?
- En effet, de quoi parle-t-on ?

Recommandations

Une analyse du risque cyber qui soit quantifiée et analysant les impacts opérationnels sur les organisations est indispensable. Elle doit être orchestrée par le *risk manager* qui doit interfacer entre

les impératifs opérationnels des fonctions et les contraintes de sécurité. Cette analyse de risque cyber doit s'appuyer sur des scénarii critiques établis par les opérationnels qui permettront le dimensionnement de l'exposition à ce risque et permettront également une meilleure prise de décision sur des politiques de réduction de risque.

La présentation de la démarche du pilote *Airbus Defence and Space SPICE* a permis d'éclairer de façon concrète comment ce processus peut être mis en place.

Il faut approfondir cette démarche pour répondre aux enjeux des TPE – TPME dans la définition de leur exposition au risque cyber et son transfert vers l'assurance.

IV.2. Pour dialoguer, savoir de quoi on parle

Les participants reconnaissaient que chacune des professions est allée aussi loin que possible, dans le cadre de ce séminaire, dans sa compréhension du risque cyber et dans son agilité créatrice pour trouver des solutions. Des discussions en séance, un élément clef est ressorti. Chaque industrie aborde le sujet avec ses propres définitions, ses propres notions sans les partager ou tout du moins sans avoir la clef de lecture des autres professionnels (assureur, industriels, experts informatiques…) Il s'avère désormais essentiel de partager le même langage pour favoriser la qualité du dialogue entre le *risk manager* et l'assureur, et aider au développement du marché de l'assurance.

Le partage de définitions communes se heurte au principe de la liberté contractuelle entre les acteurs. Ainsi, tout en respectant le droit de la concurrence, une compilation de définitions existantes permettrait de dégager des notions partagées par le plus grand nombre.

Afin de souscrire un contrat d'assurance les parties doivent s'accorder sur des notions élémentaires : quel risque assure-t-on ?, quel fait générateur ?, quelle limite de garantie ? … Or, il n'existe pas d'argus du cyber qui permettrait de savoir à quelle catégorie appartient son système, son environnement par rapport à tel volume de données…

De quoi parle-t-on ?

Chacun parle un langage qui lui est propre dans le cadre de sa profession.

Les définitions utilisées dans les contrats d'assurance sont aujourd'hui essentiellement une compilation des définitions rédigées par les assureurs et réassureurs qui, dans la liberté contractuelle qui est la leur, ont rédigé des définitions qui ne s'adaptent pas forcément à ces nouveaux risques. Ils ont pu dupliquer des définitions de risques, de garanties...pour des événements connus et maîtrisés (l'incendie, la responsabilité civile, le bris de machine...) mais qui ne s'adaptent pas nécessairement aux risques cyber.

De plus, appréhendant de nouveaux paradigmes d'assurance, chaque entreprise d'assurance et de réassurance a développé des définitions, reflet de leur expérience de politique de souscription et d'indemnisation passée.

Par ailleurs la législation propre aux risques cyber se développant tant à un niveau national qu'européen, les références passées ne sont plus forcément adaptées à ces nouveaux risques.

Les limites sont les suivantes :

L'insécurité juridique est une question qui peut être posée car les définitions sont diverses et aucun langage commun n'a spontanément émergé. Les assurés s'interrogent sur la sécurité juridique des contrats. L'accord des parties sur le périmètre des définitions peut juridiquement être remis en cause. Le contentieux est possible. En cas de conflit ou de réclamation, le juge peut apprécier les clauses d'un contrat qui déclenchent la garantie, les frais et les pertes indemnisables. Le juge peut dire qu'un contrat d'assurance dénature la notion juridique, que le fait générateur en l'espèce ne ressort pas du pénal, etc. Par nature, le contractuel n'est pas totalement sécurisé devant une juridiction car il est apprécié au regard de notions légales et de principes généraux qui lui sont supérieurs.

Par ailleurs, le cyber étant par nature transfrontalier, des problématiques de territorialité et d'application de telle ou telle loi nationale ou supra nationale peuvent se poser. Ainsi, la territorialité de la garantie dans le contrat d'assurance cyber reste à être clarifiée. Cet élément constitue un risque en soi. Prenons deux exemples transatlantiques qui illustrent ces difficultés futures liés à l'imbrication du numérique :

- Le droit évolue, et, à l'heure où nous écrivons, le Parlement français étudie la possibilité d'insérer un amendement dans le projet de Loi pour une République numérique lequel pourrait permettre d'engager des *class actions* en matière d'atteinte aux données personnelles. Le droit européen évolue également. Il est désormais posé en Europe le principe du choix de la juridiction où ester en justice : là où dans le territoire de l'Union européenne le droit et la jurisprudence sont les plus favorables.
- Du fait de la dématérialisation de l'objet cyber, dans la mesure où les États-Unis ont créé l'internet, ses réseaux et en maîtrisent la gouvernance, ils souhaitent y conserver la liberté de manœuvre qu'elle leur offre sur le plan stratégique. L'État américain considère qu'il peut exercer un droit de suite et qu'il peut pousser sa juridiction à tous ceux qui utilisent ces éléments-là selon l'adage : est maître des lieux celui qui les organise. Les Juridictions américaines sont également un levier de l'*Economic Warfare* dans laquelle sont engagés les acteurs américains. Ainsi le montant des sommes réclamées par les tribunaux américains est conséquent en cas de litige. Certes, la cour de Justice européenne dans son arrêt *Safe Harbor* (décision du 6 octobre 2015) a invalidé la décision par laquelle la Commission européenne avait constaté que les États-Unis assurent un niveau de protection suffisant des données à caractère personnel européennes transférées. Cela ouvre une période d'incertitude juridique.

Le dialogue est compliqué également parce que le vocabulaire utilisé pour le risque cyber technique, assurantiel et juridique est différent. Ou bien, la sémantique utilisée est la même mais elle exprime des réalités techniques, assurantielles et juridiques (régimes) qui ne se recoupent pas exactement. Le continuum des catégories et des définitions devrait être élaboré d'une profession à l'autre.

Quel est l'intérêt de produire des définitions médianes ?

Les Britanniques se sont engagés dans un tel exercice dans le cadre d'un Partenariat Privé Public de mise à plat de définitions médianes. Il faut ainsi noter l'effort conduit par les Britanniques du *Cambridge Center for Risk Studies*[10], pour proposer des définitions médianes, communes aux parties prenantes. Sans porter atteinte au droit de la concurrence national et européen, un exercice des définitions amont permettrait de partager une meilleure connaissance commune du sujet et de dérisquer la contractualisation des définitions contractuelles au niveau du marché. Sur les variations des définitions en aval pourrait s'exprimer la liberté contractuelle dans de meilleures conditions de sécurité juridique en cas de contentieux.

Un premier effort de compilation des définitions de ce que recouvre le risque cyber a été conduit dans le cadre du séminaire. Il a donné lieu à l'élaboration d'un tableau (voir extrait ci-dessous) qui met en exergue les divergences de définition concernant un même objet. Ce travail doit être poursuivi. L'annexe 7 fournit un premier glossaire général non consolidé.

L'hétérogénéité des définitions contractuelles et l'éventuel défaut de sécurité juridique constituent un frein au développement du marché de l'assurance.

Pourquoi se poser cette question aujourd'hui ? Certains participants se sont interrogés sur la pertinence de l'assurance de choses (assurance de dommages et de responsabilité) pour couvrir parfaitement ce nouveau type de risques. On propose d'assurer un objet « cyber » qui n'est pas juridiquement clairement défini (la donnée/la data, le logiciel, le robot, etc.) et dont la théorie économique de la quantification n'est pas aboutie. On lui demande d'indemniser : de payer pour quelque chose qui n'existe pas. Comment indemniser lorsque l'objet n'a pas d'existence, de réalité de vérité juridique et qui plus est n'est pas quantifiable ?

Les contrats d'assurance concernant le risque cyber ne peuvent pas s'appuyer aujourd'hui sur un droit du numérique ou informationnel cohérent et stable car il n'existe pas encore. Le droit ne s'est pas saisi de cette question dans son ensemble. Il n'a pas suivi dans ce domaine (comme dans d'autres) le développement de la technique. Or, pour certains participants au séminaire, ses principes fondamentaux (applicable dans le monde physique) ne se déclinent pas automatiquement pour répondre aux particularités du fait numérique immatériel et de la réalité technique de la cyber sécurité.

Le droit a abordé au mieux cette question de façon parcellaire, en silo, par profession sans jamais construire les fondations du droit du numérique. On assiste cependant à une production juridique et réglementaire importante aux niveaux national et européen (le développement de la Société de l'Information est une compétence communautaire).

[10] Cambridge Risk Framework, Cyber Accumulation Risk Management : Cyber Insurance exposure data schemaV1. https://cyberpolicymagazine.com/media/k2/items/cache/2cebfdae7a8ea5d691033c085990a9d4_XL.jpg

TERMS	DEFINITIONS 1	DEFINITIONS 2	Assureur XXX	Definitions Cyber YYY	Definitions Cyber ZZZ	Assurance FFF	Definitions AAA	Courtier	Juridique	remarques	complément
Computer Systems	"Computer Systems" means computers and associated input and output devices, data storage devices, networking equipment, and back up facilities: 1. operated by and either owned by or leased to the Insured Organization; or 2. operated by a third party service provider and used for the purpose of providing hosted computer application services to the Insured Organization or for processing, maintaining, hosting or storing the Insured Organization's electronic data, pursuant to written contract with the Insured Organization for such services.	Computer System means computer hardware, software, firmware, and the data stored thereon, as well as associated input and output devices, data storage devices, networking equipment and Storage Area Network or other electronic data backup facilities.	Planning, engineering, development, delivery and installation of IT systems, software and hardware for technical, scientific and commercial data processing.	Computer system means computer hardware, software, networks, networking equipment, applications, associated electronic devices, electronic data storage devices, input and output devices, and back up facilities operated by, owned by, leased to the Insured or for which the Insured provides technology services to others for a fee by written contract for such purposes.	système d'information : Ensemble composé d'un ou plusieurs ordinateurs en réseau, de périphériques (y compris de dispositifs physiques de stockage ou de sauvegarde de Données Numériques), de logiciels et d'installations de réseau, coordonné de manière à permettre le traitement et l'échange d'informations. Est inclus dans la présente définition tout système d'information accessible par internet, intranet, extranet ou réseau privé virtuel. Système d'information de la Société souscriptrice : un système d'information : - que la société souscriptrice loue, exploite ou dont elle est propriétaire; ou - qu'un prestataire exploite pour le compte de la société souscriptrice.	Tout système de traitement automatisé de données dont l'assuré est propriétaire, tel que visé par les articles 323-1 à 323-3 du Code pénal (ou toute législation étrangère équivalente).	SYSTEME INFORMATIQUE a) Le matériel et les équipements informatiques, les logiciels et leurs composants qui font partie intégrante d'un système ou d'un réseau accessible par internet ou le réseau intranet ou connecté à une plateforme de stockage ou tout autre appareil périphérique appartenant à, contrôlé, exploité ou loué par la société souscriptrice; b) Tout ordinateur ou tout système électronique d'un tiers (y compris tout ordinateur, tout téléphone portable ou toute tablette numérique appartenant à ou sous le contrôle d'un préposé de la société souscriptrice) utilisé pour accéder au système informatique ou aux données stockées dans le système informatique; c) Les services de cloud utilisés par la société souscriptrice. L(ES POINTS b) ET c) CI-DESSUS NE SONT PAS APPLICABLES A LA « GARANTIE INCIDENT TECHNIQUE » LORSQUE CELLE-CI EST SOUSCRITE), ET A LA « GARANTIE PERTES D'EXPLOITATION SUITE A UNE INTERRUPTION DU SYSTEME INFORMATIQUE » (LORSQUE CELLE-CI EST SOUSCRITE). 63. SYSTEME INFORMATIQUE DU PRESTATAIRE D'EXTERNALISATION Les matériels ou équipements informatiques, les logiciels et leurs composants qui font partie intégrante d'un système ou d'un réseau accessible par internet ou le réseau intranet ou connecté à une plateforme de stockage ou à tout autre appareil périphérique appartenant à, contrôlé, exploité ou loué par une prestataire d'externalisation.	Système informatique : Ensemble des ressources informatiques comprenant, notamment : les matériels informatiques, progiciels, logiciels, bases de données et périphériques, équipements, réseaux, installations électroniques de stockage de données informatiques, y compris les Données. Le Système informatique de l'Assuré s'entend comme celui : • appartenant à l'Assuré et/ou; • loué, exploité ou détenu légalement par l'Assuré au titre d'un contrat avec le détenteur des droits sur ledit système et/ou ; • exploité pour le compte de l'Assuré par un Tiers dans le cadre d'une relation contractuelle et/ou ; • contractuellement mis à disposition de l'Assuré dans le cadre d'un système mutualisé.	S ystème informatique : Tout système de traitement automatisé de données dont l'assuré est propriétaire, tel que visé par les articles 323-1 à 323-3 du Code pénal (ou toute législation étrangère équivalente).	Depuis 1986, nous traitons en France **la sécurité des systèmes d'information et non pas la sécurité informatique**. Un système d'information, c'est de l'informatique, des procédures et des hommes. Les américains avaient fractionné cela en COMSEC, COMPUSEC, TRANSSEC, etc. avec l'objectif, quand nous avons mis au point les critères de sécurité européens ITSEC (qui ont abouti aux critères communs) de nous empêcher de traiter de la cryptographie. Les bonnes définitions sont les suivantes. **Sécurité des systèmes d'information** Ensemble des mesures techniques et non techniques de protection permettant à un système d'information de résister à des événements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. **Système d'information** Ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) permettant de traiter et de diffuser de l'information. http://www.ssi.gouv.fr/publication/la-strategie-de-la-france-en-matiere-de-cyberdefense-et-cybersecurite/	**Information system** Organised set of resources (hardware, software, personnel, data and procedures) used to process and circulate information. **Information systems security** All technical and non-technical protective measures enabling an information system to withstand events likely to compromise the availability, integrity or confidentiality of stored, processed or transmitted data and of the related services that these systems offer or make accessible

Figure 2 – Exemples de définitions *computer systems* / système informatique.

Comment pouvons-nous atteindre l'objectif : parlons des mêmes choses !

Pour être assuré, le risque doit être assurable : quelles sont les conditions de l'assurabilité du risque cyber ?, quelle définition donne-t-on au risque ?, comment peut-il être quantifié ? Lorsque ces deux dernières conditions sont réunies, le risque cyber devient assurable, « contractualisable ». Les conditions de développement d'un nouveau marché de l'assurance sont alors atteintes. Les professionnels du risque que sont les assureurs vont pouvoir apporter des réponses aux demandes de couvertures des *risk managers*.

Il s'agit de traduire la dimension technique du risque cyber en dimension contractuelle au croisement des notions assurantielles et juridiques. Cette action doit s'inscrire dans une approche transdisciplinaire pour faire le lien entre la technique cyber et son vocabulaire pour matérialiser en droit ce phénomène.

La logique d'un point de vue juridique voudrait mettre de l'ordre dans les notions juridiques avant de contractualiser. Deux corpus juridiques sont à adresser : ce dont on parle et qui va être assuré et la manière de l'assurer. Le contrat d'assurance étant une règle relative à l'indemnisation de quelque chose d'immatériel, l'autre aspect concerne l'immatérialité proprement dite.

Un exercice de rédaction, de définition et de catégorisation est donc nécessaire. La difficulté est accrue par l'internationalisation du cyber risque qui doit trouver son équilibre entre les différents droits, principalement européens et américains. L'Europe doit s'emparer rapidement de ces sujets afin de ne pas subir l'emprise américaine voir anglo-saxonne. Ces travaux juridiques pourraient aboutir à une proposition de directive européenne ou de règlement qui sont le mode juridique le plus approprié pour fondre ou relier les grands systèmes de droit de l'Union (FR, All, RU).

Le système d'information et les données

Il s'agira donc, par exemple, de définir le système d'information (SI). Quelle pourrait être ainsi la définition médiane d'un SI qui aurait confirmé que les éléments techniques sont alignés à un degré de granularité nécessaire avec les notions communes et partagées de gestion du risque et assurantielles lesquelles doivent émerger d'un socle juridique solide de catégories juridiques qui matérialiseront l'objet et permettront sa qualification ?

Comment faut-il comprendre le périmètre du Système d'Information sur lequel va s'appliquer le contrat d'assurance ? Dans la perspective de l'assurance, les choses étaient simples lorsque l'informatique était localisée dans le même environnement – dans le donjon du château fort[11] – les garanties informatiques *tous risques* fonctionnaient bien. Désormais, avec la fin du système à périmètre défini d'un point de vue technique et assurantiel, quel est le début et la fin de mon SI ? Au sens des ISO 270XX ? Dois-je considérer l'application de mon serveur avec les données dans mon serveur ? Ou bien mon SI se situe-t-il au-delà de mon serveur ? Dans la messagerie, dans mon CRM (Customer Relationship Management), dans mes données de mes salariés (bulletins de salaires gérés

[11] Le *memento pour la défense en profondeur appliquée aux systèmes d'information* s'applique mieux à des architectures centralisées non déportées, en tout ou partie, dans le Cloud (infonuagique)
voir http://www.ssi.gouv.fr/uploads/IMG/pdf/mementodep-v1-1.pdf

par ADP CGI). Le SI peut aller dans le BYOD du salarié ? Dans le Cloud ? Si seul le système de traitement de données dont le client est propriétaire est assuré, qu'en est-il de données qui seraient situées dans un SI dont le client n'est pas propriétaire (Cloud, ou SI d'un sous-traitant) mais dont le client du contrat d'assurance est responsable car il est responsable de la sécurité en tant que maître du traitement au sens des articles 34 et 35 Loi 1978. L'article 35 stipule en effet, la responsabilité sur les données à caractère personnel y compris dans les environnements sous-traitant / extérieur (et L 226-17 du code pénal).

Où se situent mes données ? Elles sont volatiles. Or, le Règlement européen, validé le 14 avril 2016, vise à instituer une coresponsabilité en fonction de l'étendue des prestations du sous-traitant, notion de coresponsabilité encore extrêmement floue. Quels vont en être les impacts pour les assureurs ?

Il serait également utile de conduire des travaux de recherche pour élaborer les fondations du droit numérique ou informationnel afin de créer une réalité juridique à la donnée informatique (qualification et quantification) et répondre aux failles du droit pour sécuriser sur un plan juridique le transfert du risque vers l'assurance. Parce qu'il était très ambitieux de refonder le droit autour de la notion de donnée informatique, des morceaux de droit ont été élaborés pour créer des normes de protection non pas par rapport à l'objet à protéger mais qui correspondaient à l'objectif de protection. Le droit a ainsi protégé les personnes au travers des données personnelles (1978), les auteurs au travers de leur création logicielle (les logiciels sont des œuvres de l'esprit), les fabricants des bases de données pour qu'ils puissent les vendre… Par à-coup, des normes de protection ponctuelle ont été développées sans jamais définir ce qu'est la donnée.

Les données ne sont pas juridiquement définies, elles sont ni qualifiées ni quantifiées. Sur des fondations solides, le marché de l'assurance pourra pleinement être créatif dans la rédaction de clauses contractuelles sans le risque, qu'au contentieux, l'édifice ne s'écroule.

Recommandations

La démarche développée en interne *Airbus Defence and Space* dans le pilote SPICE – *Scenario Planning for Identification of Cyber Exposure* – qui permet au *risk manager* de connaitre son exposition au risque cyber pourrait être proposée comme base de réflexion pour produire une analyse quantifiée de l'impact business et financier lié au risque cyber pour son transfert vers l'assurance et définir un standard.

Il serait opportun de conduire un exercice de compilation des définitions contractuelles et réglementaires pour développer une connaissance commune et médiane des définitions sur le modèle du *PPP Britannique Cambridge University*.

Il serait utile d'identifier les lacunes du droit du numérique pour renforcer la sécurité juridique dans les contrats d'assurance. Il faut répondre aux questions suivantes : de quoi parle-t-on (créer le continuum et la convergence entre les éléments techniques, assurantiels et juridiques pour définir le périmètre du contrat, les champs de responsabilité et leurs limites) ?

Et enfin, créer la qualification juridique de la donnée informatique et les éléments permettant la quantification de sa valeur en vue de son transfert vers l'assurance, est indispensable.

V. Les Catégories Communes

Verrous à lever

Quels pourraient être les catégories communes et factuelles de l'analyse de l'exposition au risque cyber ?

Est-il possible de créer des catégories élémentaires du risque cyber comme dans un le tableau de Mendeleïev ?

Une fois le travail de définitions médianes conduit, le chantier des catégories communes peut être ouvert et nous pouvons répondre aux questions suivantes :

- Quels sont les catégories communes élémentaires constitutives des scenarii d'attaque cyber ?
- Quels sont les faits générateurs dans le contrat d'assurance ?
- Quel est le type de risque, les impacts et les mesures d'impact ?
- Quelles sont les informations à obtenir et à réunir du point de vue de l'assureur ?
- Quels sont les métriques à utiliser ?
- Comment les associer ?
- Quelles sont les définitions à disposition ?

V.1. La gestion du scénario au travers des catégories communes élémentaires

Une première étape a été franchie lors d'une session de travail supplémentaire de *reality check*. Il est en effet possible de jouer les catégories élémentaires du risque cyber inspiré du tableau de Mendeleïev pour décrire le scénario d'une attaque cyber.

En effet, l'analyse de risque cyber telle que présentée précédemment est une analyse qui est par nature spécifique à chacune des entités du fait de la spécificité de leur activité, de leur structure, localisation etc…

L'enjeu est donc de pouvoir trouver un référentiel commun à une multitude d'analyses spécifiques. Nous faisons le parallèle avec les molécules chimiques qui sont infinies dans la nature et qui pourraient être assimilées au scénario d'analyse de risque. Toutes ces molécules sont décomposables en un nombre fini d'éléments atomiques rassemblés dans le tableau de Mendeleïev qui est le référentiel commun de la chimie.

Par analogie, notre réflexion a porté sur la définition de catégories de risques élémentaires. L'objectif étant que chaque scénario puisse être décomposable en une combinaison de ces catégories élémentaires de risque. Il s'est agi de définir les catégories en fonction de leur complexité croissante : molécules, atomes et leurs combinaisons en évitant l'explosion combinatoire. Le scénario devient ainsi une suite d'évènements constitués d'éléments prédéfinis auxquels pourront être associées des métriques objectives. Cette approche fournit un système logique cohérent plutôt qu'une liste exhaustive de scénarii. Les cellules de la matrice sont la conjonction d'un fait générateur dommageable et d'une conséquence qui peut être appelée garantie. Les colonnes sont les faits générateurs et les lignes les garanties.

Cela nous a amené à définir une matrice dans laquelle on définit ces familles de faits générateurs et de garanties de telle manière que les cellules de cette matrice sont les catégories élémentaires (les éléments du tableau de Mendeleïev).

Concernant les faits générateurs, nous avons défini des ensembles : six catégories – évènements causant des dommages accidentels, évènements causant des dommages physiques par malveillance, les actes de malveillance informatique, les actes d'erreur humaine et actes de fraude.

Les colonnes apportent un niveau de détail supplémentaire.

En termes de conséquences, nous avons considéré des conséquences subies par l'assuré et ensuite des conséquences relatives au tiers ainsi que les problématiques de protection juridique et de sanctions infligées.

Chacune de ces lignes est détaillée de façon à être la plus explicite possible.

La réflexion s'est engagée autour des questions suivantes : Comment procéder pour obtenir des résultats comparables d'une entreprise à l'autre ? Comment définir les éléments transverses ainsi que les catégories élémentaires en évitant l'écueil de la complexité des combinaisons. La crédibilité de l'analyse réside dans l'évaluation quantitative de l'exposition reconnue par les opérationnels, faisant l'objet d'un consensus et comprise par le marché.

La méthode adoptée est la suivante : il s'est agi d'identifier des causes connues de tous, ayant des interactions minimales pour évaluer des conséquences avec l'objectif d'obtenir des éléments les plus unitaires possible.

Le *risk manager* peut ainsi utiliser cette matrice pour traduire ses scénarii d'exposition en une combinaison de faits générateurs et de garanties qui sont les catégories élémentaires. Chaque catégorie élémentaire quantifie l'exposition financière relative à ces scénarii. Chaque scénario peut ainsi être décomposé en catégories élémentaires. Dans cette décomposition, le montant financier relatif à ces scénarii va pouvoir être associé à chaque cellule impliquée.

De cette manière, sera créé ce référentiel commun d'exposition qui permettra au *risk manager* d'appréhender ses besoins. Il sera ainsi en mesure de dialoguer avec le marché. Dans la mesure où il connait à la fois la nature de son risque et son montant financier, il est plus à même de pouvoir exprimer son besoin à l'assureur. L'assureur, sur la base de ce référentiel partagé, peut analyser relativement à d'autres clients du même secteur, de la même zone etc. ce besoin de façon à y apporter une réponse appropriée.

Le tableau, en figure 3, présente cette grille vierge qui permet au *risk manager* d'analyser la couverture assurantielle de son organisme

Périmètre Cyber sur le marché français		Faits générateurs dommeageables / Garanties	Evénements causant des Dommages physiques accidentels				Evénements causant des Dommages physiques par malveillance (actes crapuleux, activisme ou terrorisme si conditions légales réunies)				Malveillance Informatique (actes crapuleux, activisme ou terrorisme si conditions légales réunies)											Erreur humaine					Fraude			
											Cyber attaques diffuses				Cyber attaques ciblées															
			Incendie	Explosion / foudre	DDO, TDC, Evénements naturels	Bris de machines	Incendie volontaire	Sabotage	Vol physique (avec ou sans effraction)	Vol physique ou dégradation d'un Bien par une cyber attaque	Usurpation d'un logiciel vérifié	Virus, vers... (codes malveillants) => perte de fonctionnement	Rançongiciel par cryptolocker	Rançongiciel sur vol de données personnelles	Rançongiciel sur vol de données personnelles	Vol de données personnelles	Vol de données confidentielles / espionnage économique	Sabotage externe	Sabotage interne (salarié ou ex salarié)	Rebot d'attaque	Intrusion et maintien dans le SI sans dommage immédiat (phi...)	Déni de service	Perte ou fichiers	Usurpation d'un logiciel endommagé	Transmission involontaire de données	Autres actions immatérielles involontaires (sans dommage matériel	Autres actions immatérielles involontaires (avec dommage matériel)	Cyber détournement de fonds	Fraude téléphonique	Vol (dans all.), escroquerie, abus de confiance, de faux, falsification de chèque	Faux ordres de Virements Internationaux - Fraude au président
Dommages subis par l'assuré (1ère partie)	Dommages matériels	Bâtiments																												
		Marchandises																												
		Matériels industriels																												
		Matériels informatiques																												
	Transport	Maritime																												
		Aérien																												
	Dommages pécuniaires	Perte pécuniaire : remboursement des fonds détournés																												
		Remboursement des rançons / sommes extorquées sous la menace																												
		Frais de recours et de poursuites																												
	Pertes d'exploitation	Perte d'opportunité																												
		Perte de marge brute / de recette																												
		Frais supplémentaires d'exploitation (pour minimiser la perte de MB)																												
		Aggravation de PE à la suite d'une décision administrative légalement prise																												
	Frais informatiques	Frais de recherche de cause: - IT : Forensic, frais d expertise, d assistance... - Mat : frais d'expertise, de recherche de cause...																												
		Frais de reconstitution de données																												
		Frais supplémentaires (travaux activité sup., gestion de crise)																												
		Conseils/ préconisations après attaque/ sinistre (remédiation)																												
		Frais d'amélioration de la sécurité informatique du SI																												
	Frais liés à une violation des données personnelles	Frais de notification aux instances administratives																												
		Frais de comparution (enquêtes administratives)																												
		Frais de notification aux personnes concernées par une violation de données personnelles																												
	frais liés au rétablissement de l'E-réputation et à la communication	Conseil en communication / Relations Publiques / Gestion de crise																												
		Nettoyage- noyage																												
		Frais de référencement																												
		Plateforme téléphonique (n° vert)																												
Protection Juridique	Protection juridique	Conseil juridique (hot line, gestion de crise)																												
		Assistances juridiques : mise en oeuvre de l'action juridique																												
		Honoraires d'avocats, d'huissiers, d'experts judiciaires																												
Dommages causés par l'assuré à un tiers (3ème partie)	Dépenses nécessaires à l'indemnisation des préjudices subis par des tiers du fait de la responsabilité civile de l'assuré	Dommages matériels aux tiers																												
		Dommages immatériels (aux tiers) consécutifs																												
		Dommages immatériels non consécutifs																												
		Dommages corporels (aux tiers)																												
		Frais de retraits / dépose / repose																												
		Défense recours																												
		RC des mandataires sociaux																												
Sanctions infligées à l'assuré	Amendes et pénalités	Amendes civiles (procédures abusives)																												
		Amendes administratives																												
		Amendes pénales																												
		Pénalités de retard (consécutifs au fait dommageable)																												
		Pénalités PCI-DSS (UNIQUEMENT pour les banques)																												
		Pénalités PCI-DSS (hors banques si applicable)																												

Figure 3 – Matrice Faits générateurs dommageables / Garanties

V.2. Les faits générateurs du risque cyber dans le contrat d'assurance

Quels sont les faits générateurs dommageables, les causes, les conséquences et les triggers du déclenchement de la couverture pour le risque cyber ?

La liste des faits générateurs dommageables construite par le groupe de travail est la suivante :

- Evénements causant des Dommages physiques accidentels
  - Incendie ; Explosion / foudre ; DDE, TOC, Evénements naturels ; Bris de machines
- Evénements causant des Dommages physiques par malveillance (actes crapuleux, activisme ou terrorisme si conditions légales réunies)
  - Incendie volontaire ; Sabotage ; Vol physique (avec ou sans effraction) ; Vol physique ou dégradation facilité par une cyber attaque
- Malveillance informatique (actes crapuleux, activisme ou terrorisme si conditions légales réunies)
  - Cyber attaques diffuses
    - Livraison d'un logiciel vicié ; Virus, vers… (codes malveillants) => entrave au fonctionnement ; Rançonnage par cryptolocker ; Rançonnage sur vol de données personnelles
  - Cyber attaques ciblées
    - Rançonnage sur vol de données personnelles ; Vol de données personnelles ; Vol de données confidentielles / espionnage économique ; Sabotage externe ; Sabotage interne (salarié ou ex. salarié) ; Relai d'attaque ; Intrusion et maintien dans le SI sans dommage immatériel (APT…) ; Déni de service
  - Erreur humaine
    - Perte de fichiers ; Livraison d'un logiciel endommagé ; Transmission involontaire de données ; Autres actions immatérielles involontaires SANS dommage matériel ; Autres actions immatérielles involontaires AVEC dommage matériel
- Fraude
  - Cyber détournement de fonds ; Fraude téléphonique ; Vol (sans effr.), escroquerie, abus de confiance, faux-usage de faux, falsification de chèque ; Faux ordres de Virements Internationaux - Fraude au président

La liste des conséquences dommageables pouvant faire l'objet de garanties, construite par le groupe de travail, est la suivante :

- Dommages subis par l'assuré (first party)
  - Dommages matériels
    - Bâtiments ; Marchandises ; Matériels industriels ; Matériels informatiques
  - Transport
    - Maritime ; Aérien
  - Dommages pécuniaires
    - Perte pécuniaire : remboursement des fonds détournés ; Remboursement des rançons / sommes extorquées sous la menace ; Frais de recours et de poursuites
  - Pertes d'exploitation
    - Perte d'opportunité ; Perte de marge brute / de recette ; Frais supplémentaires d'exploitation (pour minimiser la perte de MB) ; Aggravation de PE à la suite d'une décision administrative légalement prise
  - Frais informatiques

        - Frais de recherche de cause: - IT : Forensic, frais d'expertise, d'assistance...- Mat : frais d'expertise, de recherche de cause... ; Frais de reconstitution de données ; Frais supplémentaires (travaux activité sup., gestion de crise) ; Conseils/ préconisations après attaque/ sinistre (remédiation) ; Frais d'amélioration de la sécurité informatique du SI
    - Frais liés à une violation des données personnelles
        - Frais de notification aux instances administratives ; Frais de comparution (enquêtes administratives) ; Frais de notification aux personnes concernées par une violation de données personnelles
    - frais liés au rétablissement de l'E-réputation et à la communication
        - Conseil en communication / Relations Publiques / Gestion de crise ; Nettoyage- noyage ; Frais de reréférencement ; Plateforme téléphonique (n° vert)
- Protection juridique
    - Conseil juridique (hot line, gestion de crise) ; Assistances juridiques : mise en œuvre de l'action juridique ; Honoraires d'avocats, d'huissiers, d'experts judiciaires
- Dommages causés par l'assuré à un tiers (third party)
    - Dépenses nécessaires à l'indemnisation des préjudices subis par des tiers du fait de la responsabilité civile de l'assuré
        - Dommages matériels aux tiers ; Dommages immatériels (aux tiers) consécutifs ; Dommages immatériels non consécutifs ; Dommages corporels (aux tiers) ; Frais de retraits / dépose / repose ; Défense recours ; RC des mandataires sociaux
- Sanctions infligées à l'assuré
    - Amendes et pénalités
        - Amendes civiles (procédures abusives) ; Amendes administratives ; Amendes pénales ; Pénalités de retard (consécutifs au fait dommageable) ; Pénalités PCI ·DSS (UNIQUEMENT pour les banques) ; Pénalités PCI -DSS (hors banques si applicable)

D'un point de vue juridique, la collecte des faits générateurs est le *trigger* de la couverture.

Certains membres du séminaire ont souhaité attirer l'attention du groupe à l'utilisation de concepts porteurs d'impacts juridiques inadaptés. Ces mêmes membres ont donné, comme exemples, les définitions du vol de donnés, fraude et sabotage qui aspirent la qualification vers des catégories de droit pénal. Le risque étant de donner un marqueur de droit pénal « national » et généralement interprété de façon stricte. Ce vocabulaire peut ne pas embrasser des situations à la marge qui sont communes dans l'environnement cyber. Par exemple, comment faire coïncider la notion de vol de données à une notion juridique racine telle que « acte illicite » entendu comme « acte illicite à l'égard de données » qui pourrait englober tout ce qui correspondrait à une appropriation et à une utilisation contraire à la volonté du titulaire de la donnée ?

Recommandations

Il s'agit de poursuivre la réflexion sur les faits générateurs afin de couvrir tous les scenarii possibles.

Autre point important, pour certains membres du groupe, les causes et conséquences dans l'acception assurantielle ne correspondent pas tout à fait aux notions juridiques de causes et conséquences. L'exercice de qualification qui devra être conduit doit porter sur un amont (sur le fait générateur) et sur un aval (la conséquence). La réflexion en amont sur la catégorisation devra être faite en ne se rendant pas prisonnier de catégories juridiques pré existantes ou pré existantes et/ou mal adaptées à l'environnement cyber.

V.3. Les métriques

Pour pouvoir quantifier le risque les assureurs ont besoin de mesures fiables et solides en provenance des assurés.

Les métriques associées au risque cyber ne sont pas consolidées par manque de modélisation économétrique. Les modèles mathématiques, statistiques etc. existent mais pas les données d'entrées pour les faire tourner. Les incidents cyber ne faisant pas encore l'objet de recensement, de remontée ou de communication, les données manquent. Les acteurs ont du mal à évaluer.

Dans le cadre du séminaire, une première réflexion a été engagée par les juristes du séminaire pour faire avancer ce sujet. Le choix s'est porté sur des métriques classiques du point du vue « finance d'entreprise » et communément acceptées par le marché de l'assurance. L'exercice a conduit à définir ceux qui pourraient être utilisés pour les dommages subis et des dommages commis aux tiers. *L'interrogation porte sur les notions de frais, coût, honoraires et prix au regard des vocabulaires juridique et comptable. « Frais » est différent de « coût » lequel peut faire naître une incertitude économique sur ce que l'on cherche à indemniser (le caractère plus ou moins direct du coût). Le coût est aussi un coût initial pour l'entreprise. Il faut ensuite ajouter une marge. L'assuré qui est victime cherche à assurer ce que cela lui a coûté en général, donc un prix lequel est le montant de ce qui est acheté/vendu à l'extérieur.*

- *Les honoraires s'entendent comme « des prestations de service extérieures » et prix doit se comprendre comme « ce qui est payé ».*
- *Effort de clarification pour « % du CA perdu sur base d'un périmètre touché et d'une combinaison du CA passé et du taux de croissance » devient «du "chiffre d'affaires compromis" (CAC), avec CAC fixé par référence au chiffre d'affaire constaté pour le périmètre d'activité affecté et à son taux de croissance prévisionnel ».*
- *Frais de gestion de stocks devient « Frais de constitution et de gestion des stocks à concurrence de [--], » pour prendre en compte la notion de constitution de stock.*
- *Perte de production … ne change pas.*
- *Sous charge … ne change pas.*
- *Augmentation des coûts de production …. Il faudrait intégrer le concept de « baisse de productivité ». Devient donc : « Augmentation des coûts de production [baisse de productivité] par modification des méthodes de production (dédommagement ?) ».*

- *Frais de justice… peut être traduit par les « amendes de toute nature, prélèvements et pénalités contractuelles ou non (les pénalités infligées à titre sanction et qui ne sont pas dans un contrat et qui peuvent résulter d'une réglementation) au titre d'une sanction obligatoire par ce que on a eu un comportement qui a été modifié par une attaque cyber qui nous met en faute.*
  - *Sanctions, prélèvements obligatoires supplémentaires et pénalités contractuelles à concurrence de [--],*
- *Frais non mais « Prix de reconstruction ou de reconstitution à concurrence de [--], » car si j'achète un service à l'extérieur c'est un prix.*
  - *Reconstruction… il faudra continuer à réfléchir.*
  - *Frais de mise en sécurité (ajout/correction de mesures de sécurité).*
- *Frais de communication de toute nature (dont communication de crise et reconstitution d'image) à concurrence de [--].*
  - *Frais de gestion de crise à concurrence de [--], n'est pas pertinente. Elle devrait disparaitre cf. la ligne frais de communication.*

- *Prix de réparation, de remplacement et de restauration des données, programmes et logiciels (incluant les coûts de recréation, de recherches et d'ingénierie). Vérifier la validité de ces concepts techniques qui couvrent le temps de la remédiation ?*
  - *Coût de protection et de prévention temporaires avant réparation définitive*.

Recommandations

Poursuivre l'effort de réflexion avec les (ré)assureurs et les assureurs sur les métriques de souscription qui permettent de répondre à la question de savoir quelles sont leurs règles de souscription qui justifient leur tarification.

Continuer à réfléchir sur les métriques d'équilibre de portefeuille pour savoir si la situation a été correctement analysée (avoir collecté suffisamment de primes) afin d'obtenir un rapport sinistre à prime suffisamment équilibré au risque d'impacter les fonds propres.

Poursuivre les travaux avec les actuaires et la profession des experts comptables et des commissaires aux comptes afin de converger.

Engager des travaux sur la quantification du risque cyber qui est nécessaire pour comprendre la métrique de souscription (la valeur) pour comprendre ce que l'on va payer et à quelle indemnisation on peut s'attendre au regard de la prime qui a été engagée.

V.4. Associer les métriques aux catégories

Une fois les éléments constitutifs des faits générateurs et des conséquences dommageables posés dans leurs grandes lignes, les membres du séminaire ont décidé de constituer le tableau de Mendeleïev permettant de croiser les causes avec les dommages subis et les dommages commis aux tiers sous tendus par les métriques associés (voir la matrice-couverture au chapitre VI).

Néanmoins, une discussion s'est ouverte sur ce que pourraient être les éléments constitutifs des métriques pour le risque cyber.

Les éléments de la discussion ont porté sur la définition de la valeur de la donnée ayant fait l'objet d'une compromission, la valorisation du préjudice, le calcul de l'impact sur les tiers, sur la connaissance par l'entreprise et par les assureurs du niveau consolidé de la menace cyber dans le cadre des OIV et au-delà ? Comme obtenir des outils descriptifs pour que chacune des parties puisse faire l'exposition au risque en fonction de scénarii opérationnels à l'instant t ? Comment définir les conditions normales, les mesures adéquates qui pourraient faire baisser l'exposition au risque imprévisible (type 0-day) ? Comment calculer la vraisemblance ou fréquence (possibilité qu'il se réalise) ? Comment calculer le risque maximum ?

A ce stade des réflexions et de l'état de l'art, ces questions restent ouvertes.

VI. La Couverture du risque cyber

Verrous Produire une définition et une qualification de l'incident cyber du point de vue de l'assuré et de l'assureur. Proposer des catégories communes et factuelles montrant qu'une organisation répond aux exigences de protection face au risque cyber. Nécessité d'un tableau des couvertures.

Produire une définition et une qualification de l'incident cyber du point de vue de l'assuré et de l'assureur est un objectif ambitieux qui dépasse le temps de ce premier séminaire. Il en est de même pour proposer des catégories communes et factuelles montrant qu'une organisation répond aux exigences de protection. Il est souhaitable de procéder par étapes. La première étant de savoir s'il est réaliste de jouer les scénarii d'une attaque cyber à partir des catégories élémentaires identifiées précédemment à partir du tableau des causes et des conséquences. L'exercice de reality check a montré que cela était possible sur la base de cas réels avérés rendus publics ou récupérés par les acteurs du marché.

La seconde étape aura été l'élaboration d'une matrice des couvertures du risque cyber à partir du premier tableau des causes et conséquences et des résultats des travaux entamés au sein de la Fédération Française d'Assurance (FFA).

VI.1. Le tableau des couvertures du risque cyber : Une matrice détaillée

Les travaux de recherche et les discussions ont conduit à la réalisation d'une matrice qui est une photographie du marché français, une synthèse de l'offre assurantielle sur le marché français. Ce tableau pourra, dans un second temps, être confronté aux périmètres assurantiels des autres pays européens et à celui des États-Unis.

Le document présenté en séance de travail montre par quel type de police d'assurance (classique – DAB – Dommage aux Biens, RC – Responsabilité Civile, Fraude), le risque cyber est couvert ou pas (SO pour sans objet). Les polices d'assurance classiques couvrent, en effet, certains risques numériques. On retrouve en colonne, les évènements qui résultent des causes initiales. Les lignes représentent les conséquences dommageables des évènements. La conjonction des deux crée des cellules qui montrent par quelle catégorie de police d'assurance le risque cyber est couvert.

Un code couleur est associé : DAB en bleu ; RC en vert ; Fraude en jaune. Les couvertures cyber sont en rouge et en rose. Le rouge indique que le risque numérique est automatiquement couvert. Les cases colorées en rouge ou rose correspondent à des couvertures délivrées par les seuls contrat cyber. Les cases en rose indiquent que ce sont des options aux contrats cyber de base. Les cases hachurées montrent qu'elles sont couvertes par deux polices. Dans ce cas, le *risk manager* doit regarder comment optimiser les couvertures. Les zones en noir identifient ce qui à ce jour n'est pas assurable au regard de la législation ou parce que le marché ne souhaite pas assurer. La majorité des

cases de la matrice montre que les polices classiques couvrent déjà le risque numérique. La matrice ne renseigne pas : le type d'attaque cyber, le type de menace (les aspects techniques évolutifs).

Cette matrice, permet au *risk manager* de rattacher son analyse de risque cyber interne à son organisation avec l'analyse de risque de l'exposition au risque cyber pour le transfert d'une partie vers l'extérieur.

Le *risk manager* visualise ainsi la structure du marché français à l'instant t. La matrice (voir 2ème tableau de l'annexe 8) est une photographie de l'existant des couvertures assurantielle pour des évènements d'origine cyber et quelle est la tendance du marché Elle soit être lue comme une analyse de la sensibilité des couvertures d'assurance pour les évènements d'origine cyber.

La réduction à deux dimensions ne doit pas masquer certaines difficultés comme, par exemple, le fait que la fraude n'est pas un événement de même nature que les autres faits.

Recommandations

La communication par les assureurs des solutions de couverture d'assurance disponibles pour répondre à l'exposition au risque cyber doit être améliorée de façon à permettre aux assurés d'être mieux informés et mieux conseillés dans leur stratégie d'externalisation de ce risque.

Les travaux de recherche proposent une représentation de la façon dont le marché français d'assurance répond aux différentes catégories de risque identifiées précédemment. Cette photo de l'état actuel de la réponse du marché permet au *risk manager* de mieux comprendre comment (voir figure 4). Elle montre comment le marché propose aujourd'hui d'adresser le risque cyber.

Il s'agit maintenant de proposer une matrice qui soit un benchmark de comparaison à l'international pour un marché qui est très concurrentiel.

Le premier tableau (figure 3) est une grille vierge permettant au *risk manager* d'analyser la couverture assurantielle de son organisme. Elle lui permet de mieux caractériser la sensibilité de ses diverses couvertures et d'articuler ses polices. Cette grille n'est pas là pour positionner des contrats dits « cyber », qu'ils soient spécifiques ou adossés à des contrats « classiques ».

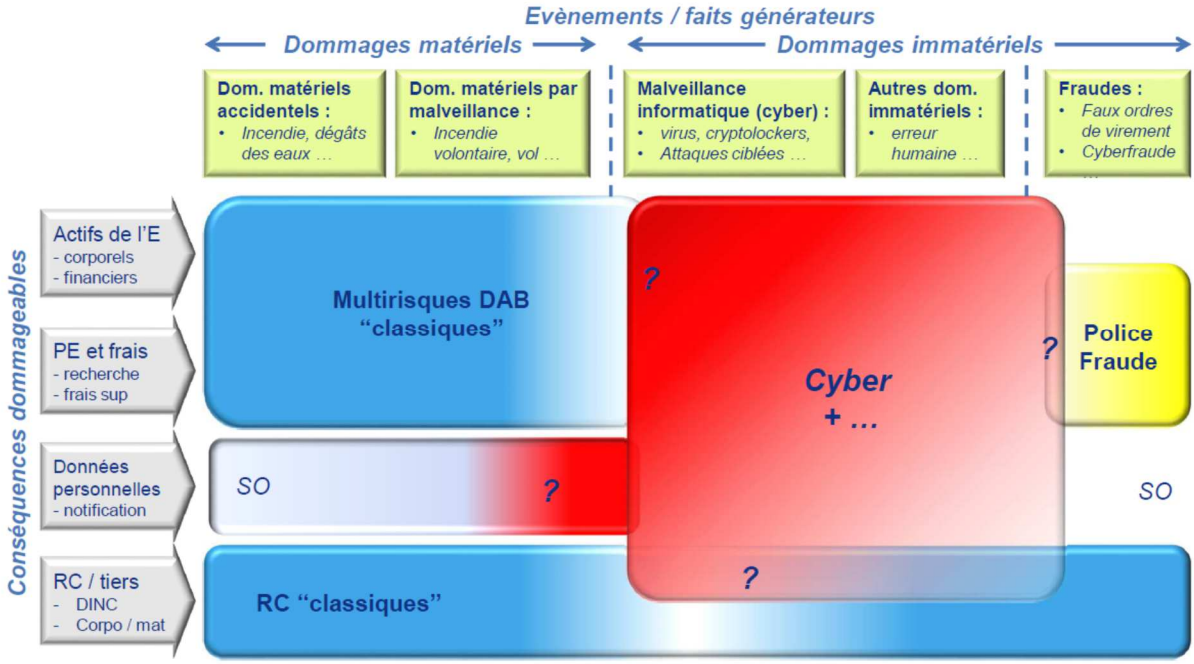
Le deuxième tableau (figure 4) fournit une photographie datée du marché français actuel. Ce calque peut être appliqué à d'autres marchés (Allemagne, Grande-Bretagne, etc.) et devra être revu au cours du temps. Il facilite le dialogue entre les divers acteurs en fixant un vocabulaire commun et en décomposant des concepts souvent trop généraux.

Figure 4 – Matrice détaillée Faits générateurs dommageables / Garanties (page suivante)

.

Périmètre Cyber sur le marché français	Faits générateurs dommeageables / Garanties	Evénements causant des Dommages physiques accidentels				Evénements causant des Dommages physiques par malveillance (actes crapuleux, activisme ou terrorisme si conditions légales réunies)				Malveillance informatique (actes crapuleux, activisme ou terrorisme si conditions légales réunies)												Erreur humaine					Fraude				Commentaires
										Cyber attaques diffuses				Cyber attaques ciblées																
		Incendie	Explosion / foudre	IDE, TOC, Evénements naturels	Bris de machines	Incendie volontaire	Sabotage	Vol physique (avec ou sans effraction)	Vol physique ou dégradation facilité par une cyber attaque	Livraison d'un logiciel vérolé	Virus, vers... (code malveillant) => entrave au fonctionnement	Ransonnage par cryptolocker	Ransonnage sur vol de données personnelles	Ransonnage sur vol de données personnelles	Vol de données personnelles	Vol de données confidentielles / espionnage économique	Sabotage externe	Sabotage interne (salarié ou ex. salarié)	Hold-up attaque	Intrusion et maintien dans le SI sans dommage immatériel (ART...)	Déni de service	Perte de fichiers	Livraison d'un logiciel endommagé	Transmission involontaire de données	Autres actions immatérielles involontaires (DEC dommage matériel)	Autres actions immatérielles involontaires (DEC dommage matériel)	Cyber détournement de fonds	Fraude téléphonique	Vol (sans effr.), escroquerie, abus de confiance, fauxnage de flux, falsification de chèque	Tous cettes de Vérements internationaux + fraude au président	
Dommages subis par l'assuré (first party)	Dommages matériels — Bâtiments	DAB	DAB	DAB	DAB	DAB	DAB	DAB	DAB	so	so	so	so	so	so	so	DAB	DAB	DAB	so	so	so	so	so	so	DAB	so	so	so	so	
	Dommages matériels — Marchandises	DAB	DAB	DAB	DAB	DAB	DAB	DAB	DAB	so	so	so	so	so	so	so	DAB	DAB	DAB	so	so	so	so	so	so	DAB	so	so	Fraude	so	
	Dommages matériels — Matériels industriels	DAB	DAB	DAB	DAB	DAB	DAB	DAB	DAB	so	DAB	so	so	so	so	so	DAB	DAB	DAB	so	so	so	so	so	so	DAB	so	so	Fraude	so	
	Dommages matériels — Matériels infomatiques	DAB	DAB	DAB	DAB	DAB	DAB	DAB	DAB	so	DAB	so	so	so	so	so	DAB	DAB	DAB	so	so	so	so	so	so	DAB	so	Fraude	Fraude	so	
	Transport — Maritime	Corps et faculté ?																								Corps et faculté ?	so	so	so	so	Exclusion du cyber (Clause 380 ou équivalents)
	Transport — Aérien	Dommage aux aéronefs, etc. ?								?																Dommages aéronefs	so	so	so	so	A l'étude
	Dommages pécuniaires — Perte pécuniaire : remboursement des fonds détournés	so	so	so	so	so	so	Fraude si pas effr	Fraude si pas effr	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	Cyber Fraude	Fraude	Fraude	Fraude	
	Dommages pécuniaires — Remboursement des rançons / sommes extorquées sous la menace	so	so	so	so	so	so	so	so	so	so	?	?	?	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	Assurabilité des rançons en cours d'analyse
	Dommages pécuniaires — Frais de recours et de poursuites	so	so	so	so	so	so	Fraude si pas effr	Fraude si pas effr	so	so	Cyber	Cyber	Cyber	so	so	so	so	so	so	so	so	so	so	so	so	Cyber Fraude	Fraude	Fraude	Fraude	
	Pertes d'exploitation — Perte d'opportunité																														Risque d'entreprise
	Pertes d'exploitation — Perte de marge brute / de recette	DAB	DAB	DAB	DAB	DAB	DAB			so	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber ?	so	Cyber ?	Cyber ?	DAB	Cyber Fraude	Fraude	Fraude	Fraude	
	Pertes d'exploitation — Frais supplémentaires d'exploitation (pour minimiser la perte de MB)	DAB	DAB	DAB	DAB	DAB	DAB			so	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber ?	so	Cyber ?	Cyber ?	DAB	Cyber Fraude	Fraude	Fraude	Fraude	
	Pertes d'exploitation — Aggravation de PE à la suite d'une décision administrative légalement prise	DAB	DAB	DAB	DAB	DAB	DAB	so	so	so	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber ?	so	Cyber ?	Cyber ?	DAB	Cyber Fraude	Fraude	Fraude	Fraude	
	Frais informatiques — Frais de recherche de cause: - IT : Forensic, frais d expertise, d assistance... - Mat : frais d'expertise, de recherche de cause...	DAB	DAB	DAB	DAB	DAB	DAB	DAB	DAB	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber ?	so	Cyber ?	Cyber ?	Cyber ?	Cyber Fraude	Fraude	Fraude	Fraude	
	Frais informatiques — Frais de reconstitution de données	DAB	DAB	DAB	DAB	DAB	DAB	DAB	DAB	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber ?	so	Cyber ?	Cyber ?	Cyber ?	Cyber Fraude	Fraude	Fraude	Fraude	
	Frais informatiques — Frais supplémentaires (travaux activité sup., gestion de crise)	DAB	DAB	DAB	DAB	DAB	DAB	DAB	DAB	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber ?	so	Cyber ?	Cyber ?	Cyber ?	Cyber Fraude	Fraude	Fraude	Fraude	
	Frais informatiques — Conseils/ préconisations après attaque/ sinistre (remédiation)	DAB	DAB	DAB	DAB	DAB	DAB	DAB	DAB	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber ?	so	Cyber ?	Cyber ?	Cyber ?	Cyber Fraude	Fraude	Fraude	Fraude	
	Frais informatiques — Frais d'amélioration de la sécurité informatique du SI																														non assurable
	Frais liés à une violation des données personnelles — Frais de notification aux instances administratives	so	so	so	so	so	so	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber	Cyber	Cyber	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	so	Cyber ?	Cyber ?	Cyber ?	Cyber ?	so	so	so	
	Frais liés à une violation des données personnelles — Frais de comparution (enquêtes administratives)	so	so	so	so	so	so	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber	Cyber	Cyber	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	so	Cyber ?	Cyber ?	Cyber ?	Cyber ?	so	so	so	
	Frais liés à une violation des données personnelles — Frais de notification aux personnes concernées par une violation de données personnelles	so	so	so	so	so	so	Cyber ?	Cyber ?	so	so	so	Cyber	Cyber	Cyber	so	so	so	so	so	so	Cyber ?	so	Cyber ?	Cyber ?	Cyber ?	so	so	so	so	
	frais liés au rétablissement de l'E-réputation et à la communication — Conseil en communication / Relations Publiques / Gestion de crise	DAB	DAB	DAB	DAB	DAB	DAB	DAB	DAB	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	so	so	so	
	frais liés au rétablissement de l'E-réputation et à la communication — Nettoyage- noyage	so	so	so	so	so	so	so	so	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Fraude	Fraude	so	
	frais liés au rétablissement de l'E-réputation et à la communication — Frais de référencement	so	so	so	so	so	so	so	so	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	so	so	so	
	frais liés au rétablissement de l'E-réputation et à la communication — Plateforme téléphonique (n° vert)	DAB	DAB	DAB	DAB	DAB	DAB	DAB	DAB	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	so	so	so	
Protection juridique	Protection juridique — Conseil juridique (hot line, gestion de crise)	so	so	so	so	so	so	so	so	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	so	so	so	
Protection juridique	Protection juridique — Assistances juridiques : mise en oeuvre de l'action juridique	so	so	so	so	so	so	so	so	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	so	so	so	
Protection juridique	Protection juridique — Honoraires d'avocats, d'huissiers, d'experts judiciaires	so	so	so	so	so	so	so	so	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	so	so	so	
Dommages causés par l'assuré à des tiers (third party)	Dépenses nécessaires à l'indemnisation des préjudices subis par des tiers du fait de la responsabilité civile de l'assuré — Dommages matériels aux tiers	DAB	DAB	RC	RC	DAB	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	
Dommages causés par l'assuré à des tiers (third party)	Dépenses nécessaires à l'indemnisation des préjudices subis par des tiers du fait de la responsabilité civile de l'assuré — Dommages immatériels (aux tiers) consécutifs	DAB	DAB	RC	RC	DAB	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	
Dommages causés par l'assuré à des tiers (third party)	Dépenses nécessaires à l'indemnisation des préjudices subis par des tiers du fait de la responsabilité civile de l'assuré — Dommages immatériels non consécutifs	DAB	DAB	RC	RC	DAB	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	
Dommages causés par l'assuré à des tiers (third party)	Dépenses nécessaires à l'indemnisation des préjudices subis par des tiers du fait de la responsabilité civile de l'assuré — Dommages corporels (aux tiers)	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC / RC ?	RC / RC ?	RC / RC ?	RC / RC ?	RC / RC ?	RC / RC ?	RC / RC ?	RC / RC ?	RC	RC	RC	RC	RC	RC	RC	RC	RC	
Dommages causés par l'assuré à des tiers (third party)	Dépenses nécessaires à l'indemnisation des préjudices subis par des tiers du fait de la responsabilité civile de l'assuré — Frais de retraits / dépose / repose	so	so	so	so	so	so	so	so	RC	so	so	so	so	so	so	so	so	so	so	so	so	RC	so	so	so	so	so	so	
Dommages causés par l'assuré à des tiers (third party)	Dépenses nécessaires à l'indemnisation des préjudices subis par des tiers du fait de la responsabilité civile de l'assuré — Défense recours	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	
Dommages causés par l'assuré à des tiers (third party)	Dépenses nécessaires à l'indemnisation des préjudices subis par des tiers du fait de la responsabilité civile de l'assuré — RC des mandataires sociaux	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	
Sanctions infligées à l'assuré	Amendes et pénalités — Amendes civiles (procédures abusives)	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	
Sanctions infligées à l'assuré	Amendes et pénalités — Amendes administratives																														non assurable
Sanctions infligées à l'assuré	Amendes et pénalités — Amendes pénales																														non assurable
Sanctions infligées à l'assuré	Amendes et pénalités — Pénalités de retard (consécutifs au fait dommageable)	DAB	DAB	DAB	DAB	DAB / RC	DAB / RC			so	Cyber / RC ?	Cyber / RC ?	Cyber / RC ?	Cyber / RC ?	Cyber / RC ?	Cyber / RC ?	Cyber / RC ?	Cyber / RC ?	Cyber / RC ?	Cyber / RC ?	Cyber / RC ?						Cyber / RC ?	Fraude	Fraude	Fraude	Pénalités contractuelles que les assureurs ne veulent pas couvrir
Sanctions infligées à l'assuré	Amendes et pénalités — Pénalités PCI -DSS (UNIQUEMENT pour les banques)	so	so	so	so	so	so	so	so	so	so	so	Cyber / RC ?	Cyber / RC ?	Cyber / RC ?	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	
Sanctions infligées à l'assuré	Amendes et pénalités — Pénalités PCI -DSS (hors banques si applicable)	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	Point de discussion !!!

Figure 5 – Matrice synthétique Faits générateurs dommageables / Garanties (page suivante)



Le risque d'origine cyber peut être couvert par plusieurs natures de couverture. Les contrats cyber branche pure, sont visualisés dans la zone rouge.

VI.2. Une proposition de matrice simplifiée (point de vue technique)

Une proposition de simplification de la matrice, au croisement des attentes du marché et de l'état de l'art évolutif de la menace cyber, a été discutée

La matrice présentée en séance de travail était très explicite-didactique-pédagogique et décrivait les techniques d'attaque actuelles. Or, demain l'état de la menace aura évolué et d'autres termes seront utilisés. Comment la matrice peut-elle suivre la mise à niveau de la menace ? Comment réfléchir à des catégories techniques chapeau qui engloberaient l'existant et permettraient d'inscrire les attaques futures sans bouleverser le tableau ? Comment créer des familles techniques de menace pour la matrice ? Faut-il réfléchir en termes de grande catégories de techniques d'attaque ? Ou doit doit-on se focaliser sur l'objectif de l'attaque : la conséquence est in fine une forme de dénis de service ? Ainsi pourrait-on remonter à une catégorie racine type « dénis de service » ?

Ce tableau (voir figure 6) permet également de mettre en évidence une double posture dans laquelle se trouve le marché une fois posé le principe « tout dommage matériel reste couvert par une police dommage même s'il est consécutif ou aggravé par du cyber. Les polices RC couvrent toute la RC cyber sauf exclusion. L'intersection des polices cyber est limitée aux dommages immatériels non couverts qui font suite à une attaque cyber ciblée. La police cyber vient en complément ».

Faits générateurs dommageables / Conséquences dommageables	Atteintes aux données sur attaque	Atteintes aux données sur erreur	Extorsion	Fraude	Entrave au fonctionnement sans dommage physique	Manipulation du produit ou du service client sur attaque	Manipulation du produit ou du service client sur erreur	Dommage materiel suite à attaque	Dommage materiel suite à erreur	Relais d'attaque
Actifs corporels	so	so	DAB	Fraude	so	so	so	DAB	DAB	so
Actifs financiers	so	so	Cyber	Fraude	so	so	so	so	so	so
Perte d'exploitation	Cyber	Cyber	Cyber	Fraude	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber
Frais informatiques	Cyber	Cyber	Cyber	Fraude	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber
Protection des données personnelles/confidentielles	Cyber	Cyber	Cyber	so	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber
E-réputation / Communication	Cyber	Cyber	Cyber	so	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber
Protection juridique	Cyber	Cyber	Cyber	Fraude	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber
Responsabilité Civile (dommages aux tiers)	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC
Amendes et pénalités	Cyber		Cyber	Fraude	Cyber	Cyber		Cyber	Cyber	Cyber

Figure 6 – Proposition de matrice simplifiée

Les contrats traditionnels (Dommages aux biens, Responsabilité Civile, Responsabilité des Mandataires Sociaux…) s'étendent pour indemniser des incidents cyber. Les polices traditionnelles vont intégrer de plus en plus de couvertures cyber.

Par exemple :

- Colonne G (Entrave au fonctionnement…) : les pertes d'exploitation et frais informatiques peuvent être indemnisés par des polices Dommages aux Biens. C'est le cas dans la police de l'assureur FM (gros acteur aux US qui vend aussi en France).
- Colonne I (Manipulation produit) : la protection juridique, e-réputation, amendes et pénalités, protection des données peuvent être indemnisées par des polices Responsabilité Professionnelle (en anglais E&O - Error & Omission).

D'un autre côté, les produits cyber spécifiques se développent.

Il est donc important de clarifier les domaines de compétence de chacun des contrats afin d'éviter pour le client de payer deux fois pour la même nature de couverture mais également afin d'éviter des recours qui risqueraient de ralentir le processus d'indemnisation.

Le périmètre des responsabilités a été un sujet de discussion important par les membres du séminaire. La réalité de la menace cyber, le phénomène de numérisation de l'économie, de digitalisation, les notions d'écosystème, de chaine d'approvisionnement, de sous-traitance hors du pays d'exploitation de la donnée montrent que dans ce domaine la chaine de responsabilité peut être importante et difficile à cerner. La spécificité technique du cyber risque oppose ses limites. Les risques de contentieux sont donc importants. Ils sont d'autant plus importants à prendre en considération au caractère déterritorialisé du contentieux cyber (juridiction-pays du contrat ? ou juridiction-pays de la victime ?). Le raisonnement selon lequel, l'assureur paye l'assuré et exerce un recours envers le responsable risque de rapidement trouver ses limites.

La couverture du risque cyber tant par des polices DAB, RC et cyber, pose la question des cumuls. Cette question est clef tant pour la (ré) assurance que pour le marché de l'assurance direct.

Elle est cruciale pour l'assurance qui doit répondre à la question comment dimensionner l'environnement contractuel au regard de l'état de l'art de la technique informatique et au regard du droit informationnel ou du numérique qui évolue. Quelles informations techniques seront demandées pour qualifier correctement les éléments ?

Recommandations

Poursuivre l'effort de simplification de la matrice des couvertures au croisement de la technique cyber et du point de vue de l'assurance.

VI.3. La matrice, vers une convergence des définitions (point de vue juridique)

Une étape vers le développement d'un langage commun est lancée. Le document est *work in progress* et fera l'objet d'améliorations ultérieures. Le séminaire a permis d'initier un effort de convergence entre les parties prenantes (assurance - la technique – les juristes).

Les définitions, lignes et colonnes commencent à converger au fil des discussions. Ou à tout le moins, les représentations différentes, les zones de non recoupement et les divergences apparaissent. Autant d'éléments qui pointent vers la prorogation des efforts pour converger.

Un exercice de renommage de certains vocables de la matrice a été conduit, qu'il s'agit de fortifier. Les juristes du séminaire ont proposé :

- Le vol de données pourrait être renommé en « appropriation illicite de données ». Car le vol en droit est une notion restrictive par rapport à la réalité des faits techniques cyber qu'il couvre. Il entraine un régime au pénal. Il faudrait remonter la notion de vol de données à une notion juridique racine telle que « acte illicite entendu comme acte illicite à l'égard de données » qui pourrait ainsi englober tout ce qui correspondrait à une appropriation et à une utilisation contraire à la volonté du titulaire de la donnée. Ensuite on déclinerait vers l'utilisation, l'appropriation…
- Les données personnelles pourraient être distinguées des données d'entreprise. Les données personnelles pourraient devenir « des données à caractère personnel » (en référence au support juridique européen qui est solide en droit). Ce qui permet d'obtenir une opposition par rapport aux données d'entreprise qui ne sont pas une catégorie de droit déjà existante mais qui est à créer.
    - Proposition : remplacer les données d'entreprise par « données à caractère d'organisation » qui reprendrait toutes les données qui sont liées au fonctionnement pour la production de bien et de service, stratégie et de R&T R&D de l'organisation. Les données de propriété intellectuelle ne superposent pas, en effet, complètement la notion de données à caractère d'entreprise. On pourrait

ainsi viser toutes les données qui ne sont pas couvertes par la PI mais qui sont mises en œuvre par l'entreprise pour sa production de biens et de service.

- L'indisponibilité totale ou partielle d'un service métier pourrait devenir « l'entrave totale ou partielle à une prestation métier » car la notion d'entrave est plus englobante que celle d'indisponibilité. L'entrave est ce que je fais. Je peux entraver sans créer une indisponibilité. Je crée ainsi une gêne suffisante pour ralentir ou empêcher la production. L'indisponibilité c'est : je mets tout en croix. C'est le résultat.
- La fraude pourrait devenir « utilisation du SI d'une organisation à des fins illicites ». La fraude à l'identité deviendrait alors « le dommage du fait de l'usurpation de l'identité ».
- Le sabotage pourrait devenir « une atteinte à un SI et à ses composantes physiques ». Le terme de sabotage en effet fait l'objet de définitions différentes et notamment dans le droit de la guerre/faits de guerre.
  - Remarque de la technique : en cyber il est possible de « saboter » de façon à endommager sans effet physique : atteinte à l'intégrité de données immatérielles par exemple.
- L'atteinte à l'image (un dommage en même temps qu'une cause) deviendrait dommage direct et indirect du fait de l'atteinte à l'image. Car l'atteinte à l'image peut causer des dommages directs (si l'image est un élément essentiel de la valeur/ du good will par exemple pour un cabinet d'avocat – prestation de services immatériels) et indirects. Idem pour la fraude à l'identité.
- Le défaut d'obligation administrative est trop restrictif. Il pourrait être modifié en « dommages directs et indirects du fait de l'entrave à la satisfaction d'une norme unilatérale ou contractuelle».

Recommandations

Poursuivre le travail de mise en cohérence de la matrice.

Poursuivre les travaux avec les actuaires et la profession des experts comptables et des commissaires aux comptes afin de converger.

Engager des travaux sur la quantification du risque cyber qui est nécessaire pour comprendre la métrique de souscription (la valeur), pour comprendre ce que l'on va payer et à quelle indemnisation on peut s'attendre au regard de la prime qui a été engagée.

VI.4. Les points d'interrogation actuellement en discussion

De nouvelles situations[12] devraient faire l'objet d'une analyse et d'une réflexion ultérieures et spécifiques – mais, dans tous les cas, approfondies - portant sur les conséquences, de fond et de procédure, des régimes législatifs et réglementaires gouvernant les polices administratives en cause, sur l'étendue des garanties d'assurance « cyber » et les modalités de leur déclenchement. Ces régimes sont récents et innovants. Ils reposent en bonne partie sur des mécanismes sans précédent en droit français. Ils constituent, dès lors, un nouvel écosystème juridique et de l'action administrative appelé à produire des effets dans l'environnement « cyber » et ses couvertures assurantielles.

Diverses questions se posent :

[12] Comme la mise en œuvre des techniques de recueil de renseignement prévues par le livre VIII du code de la sécurité intérieure ou des décisions administratives de blocage et de déréférencement des sites à caractère terroriste prises en application de la loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme.

- La rançon (le *ransomware*). Une étude est menée en interne FFA. Ses conclusions seront intégrées aux travaux plus tard. D'un point de vue technique et juridique, attribuer la responsabilité du *ransomware* est difficile.
- La fraude. L'intersection polices fraude avec le cyber mérite d'être éclaircie. La réduction à deux dimensions ne doit pas masquer certaines difficultés comme, par exemple, le fait que la fraude n'est pas un événement de même nature que les autres faits générateurs.
- Frais de notification. Le périmètre de l'assurabilité des frais de notification qui auraient une origine matérielle causant un dommage immatériel doit être étudié. Il faudra, en effet, notifier auprès des personnes que leurs données personnelles ont fait l'objet d'un vol – une compromission dont on ne connait pas la nature exacte (dommage immatériel) suite à un vol d'un ordinateur portable (dommage matériel). Comment établir une extension au contrat ?
- Le cyber terrorisme. De même, faut-il intégrer dans le tableau le risque du cyber terrorisme dès à présent ? Est-il envisageable de traiter le cyber terrorisme au regard des faits et du constat du sinistre et non pas au regard du fait générateur (par analogie avec les catastrophes naturelles) une fois que l'évènement a été qualifié de « terroriste » ? Aux États-Unis, ce risque est couvert dans la police sous-jacente. Mais en Europe, la majeure partie des polices exclue les actes terroristes (sponsorisés par des États).

Sur trois autres points, faisant l'objet d'appréciations différentes, une discussion doit être ouverte :

- Les amendes : seules les amendes civiles sont actuellement assurables.
- L'assurabilité des rançons : une question à définir au niveau européen. De leur côté, les britanniques y sont opposés.
- PCI-DSS : sur ce sujet technique, il n'y a pas de convergence aujourd'hui.

VII. Informations de Souscription

Verrous

En l'absence de statistiques de marché et au vu des couvertures existantes, comment créer les conditions générales d'un dialogue de confiance entre l'assuré et l'assureur ? Comment définir les conditions d'un dialogue de confiance entre l'assuré et l'assureur ? Quelles en sont les conditions ?

Le marché a-t-il besoin de définir des tiers de confiance qui permettraient la collecte, la validation et l'anonymisation des données permettant ensuite l'élaboration de modèles ?

Peut-on réfléchir à la création d'un organisme paritaire définissant le contenu et la validation d'une formation qualifiante d'Experts d'assurance cyber ?

VII.1. La confidentialité dans le dialogue

La question posée était de savoir quelles étaient les informations de souscription nécessaires pour cadrer le dialogue et permettre qu'il ait lieu : réunir les conditions de sa réalisation. Et s'il fallait le cas échéant élaborer un catalogue. L'AMRAE devait fournir des exemples de questionnaires.

Les informations de souscription

Pour le *risk manager* les questions posées ont peu à voir avec son interrogation principale : comment l'organisation est-elle protégée ? Il y a souvent confusion entre l'exposition de l'informatique et l'exposition de l'organisation informatisée alors que cette dernière est clef dans l'approche de son risque cyber.

Peu de questionnaires l'abordent. Certes, l'assureur doit poser des questions à l'assuré qui constituent pour lui des éléments déterminants de sa souscription, mais il n'aborde pas le sujet au fond.

Le questionnaire n'est pas non plus assis sur aucune table de calcul et aucune statistique. Il n'est pas rattaché à des métriques permettant de calculer des risques, le ratio des risques à prime qui est l'obligation de conformité des assurances.

Il ressort des premiers travaux menés par l'AMRAE sur la remontée des informations de souscription dans le domaine du cyber risque, les contraintes suivantes :

Les entreprises sont peu enclines à s'exprimer sur leur exposition au risque cyber. Celles dont l'activité est de nature sensible, voire de souveraineté, conservent une attitude prudente et communiquent seulement à haut niveau.

L'AMRAE constate le manque d'information sur le positionnement des entreprises de taille intermédiaire. Certaines PME parlent plus ouvertement que d'autres (PME high tech). Certains groupes et notamment les banques s'expriment mais ils le font sur la partie du risque cyber pour laquelle la réglementation leur impose des règles précises.

Le partage d'information, s'il a lieu, ne se fait qu'après la signature d'un accord de confidentialité entre l'assureur, le courtier et l'assuré.

Le questionnaire était la méthode la plus simple pour souscrire notamment sur le segment des TPE PME ETI. Mais, de plus en plus souvent, la formule du questionnaire semble rejetée par le client qui ne souhaite plus

répondre à une énième liste de questions (cf. audits de sécurité informatique, etc.) d'autant plus que ces dernières sont perçues comme intrusives.

De plus, tel que formulé, le questionnaire est souvent inadapté à la situation des groupes multinationaux (plusieurs pays, quel périmètre à l'intérieur de l'entreprise ...) mais aussi aux PMEs. Ces dernières ne se sentent pas concernées. Elles ne peuvent pas répondre aux premières questions posées si elles ont externalisé la gestion de leur SI, si elles ne sont pas propriétaires de leur réseau informatique, ni de leur flotte d'ordinateur et si une très grande partie de leurs données se situent chez un hébergeur.

La demande de l'assureur qui a besoin d'une cartographie du SI devient alors sans fondement.

Sur le périmètre des grands risques, le dialogue avec le marché se fait donc généralement au travers de *road shows*. Les *risk managers* présentent leur politique générale de gestion du risque cyber en interne entreprise. Le DSI et le RSSI démontrent qu'ils font le nécessaire en matière de sécurité des SI (*good will*). L'entreprise répond par oui ou par non aux questions du marché. Aucune information de nature critique n'est échangée sur les vulnérabilités, les outils, les choix des investissements et la gouvernance du risque… Rien de spécifique, que du générique.

Peu de documents internes entreprise sont laissés au marché.

Le constat est que les assureurs aidés par le courtier répondent aux besoins du client sur la base de très peu d'informations échangées. En retour, le manque d'information échangée n'offre que peu de garantie d'être couvert en cas de sinistre par le marché.

Le constat

Le marché se contente de cette situation actuellement.

Le niveau d'information échangé est donc perfectible mais encore faudrait-il que les organisations disposent en interne des informations sur leur niveau d'exposition au risque cyber pour qu'elles puissent échanger (sous une forme qui reste à déterminer).

La première condition du dialogue reste que chaque organisation connaisse sa propre exposition (à l'exemple de la démarche de type SPICE).

Il s'agit d'articuler la liberté des acteurs et la nécessité de proposer une démarche cohérente et efficace pour créer les conditions d'un dialogue entre l'entreprise (le *risk manager* porteur des éléments du DSI et du RSSI) et le marché. Néanmoins, un cadre minimum pour échanger des informations de souscription – un standard à minima serait utile, dans le respect des règles du droit de la concurrence et de la liberté pour chaque acteur d'appréhender le risque de la manière qu'il souhaite.

Recommandations

Avoir un langage commun et à partir de celui-ci avoir une métrique suffisamment objectivée et partagée.

L'ensemble des acteurs convient qu'il faut améliorer le dialogue pour que ce dernier s'ouvre sur les incidents (remontée d'information – *Big Data*).

Trouver un canal pour permettre le dialogue pour que les futurs assurés aient une meilleure visibilité, pour développer une base qui permette une étude actuarielle sur l'exposition réelle, une base quantitative qui serve à toutes les parties prenantes. Quel rôle pour la puissance publique ?

Engager une réflexion pour les TPE et PME d'un côté et pour les grands groupes de l'autre concernant la nature, le niveau nécessaire et les garanties d'informations de souscriptions dont a besoin le marché.

Travailler avec les actuaires qui savent de quel type d'information ils ont besoin.

Travailler avec les *Chief Data Officers* et les *Digital Officers*.

VII.2. La gestion de la partie sinistre

Les données informatiques, les systèmes d'informations, sont désormais au cœur des stratégies d'entreprises et des préoccupations des États.

Le législateur s'est donc naturellement emparé du sujet (Loi de programmation militaire en 2013) et impose des contraintes de confidentialités aux Opérateurs d'Importance Vitale.

Au-delà de cette « confidentialité légale », l'enjeu stratégique du cyber génère également des règles de confidentialités strictes au sein des entreprises.

Cette confidentialité associée aux risques cyber, peut apparaitre comme contradictoire avec les règles d'indemnisation des entreprises d'assurance.

Les assureurs ont déjà été amenés à gérer cette apparente contradiction dans d'autres domaines (incendie de sites sensibles, global de banque….). Pour que ces enjeux de confidentialité ne posent pas de difficultés au jour du sinistre, la transparence dans le dialogue assuré/assureur est primordiale.

Une fois informé des contraintes des uns et des autres, il appartient alors aux parties de convenir dès la souscription du contrat des modalités spécifiques de gestion du sinistre. Cela est d'autant plus important si les contraintes sont d'ordre légal (OIV, confidentiel défense, …) de façon à ce que le contrat d'assurance combine ces contraintes opposables à l'assureur et les obligations légales qui pèsent sur l'assuré de justifier de la réalité et du montant de son préjudice pour pouvoir être indemnisé en application du principe indemnitaire.

Le rôle de l'expert apparait également comme clef dans la gestion des sinistres cybers. La confiance dans l'expert est d'autant plus importante qu'il est amené à connaitre d'informations sensibles.

Une fois le sinistre survenu, l'expert d'assurance analyse la police et la réalité du préjudice pour déclencher la garantie et proposer une indemnité. Son rôle est d'aider les parties à la bonne résolution du sinistre.

Pour mener à bien sa mission dans un environnement hautement sensible de confidentialité des données, les différentes hypothèses de recours aux experts doivent donc être prévues en amont dans le contrat.

Recommandations

Il y a un besoin de clarification. N'y-a-t-il pas là un domaine où l'assureur peut apporter du service en accompagnement ou en gestion de crise qui donne une plus grande validité à son offre[13] ?

VII.3. Les conditions de la confidentialité, le rôle de la puissance publique

Que peut proposer la puissance publique pour **développer la confiance pour l'échange d'information de souscription** ? Que peut-elle proposer **pour assurer la confidentialité** : quel rôle de la puissance publique, quelles propositions pour l'avenir ? Quelles pourraient être les moyens que l'ANSSI pourrait proposer pour fournir le cadre de confidentialité nécessaire aux échanges entre assuré et assureur ? Est-ce, par exemple, dans la qualification d'acteurs certifiés ? Ou bien dans des espaces de partage d'information spéciaux ? Ou bien dans l'examen des sinistres ? Comment gérer les déclarations des sinistres et leur règlement : quelles sont les compétences techniques nécessaires pour vérifier la véracité des pertes et évaluer leur montant ?

La puissance publique ne souhaite pas être en coupure dans la relation entre l'assuré et l'assureur (reconnaissance du caractère commercial de la relation).

- **La puissance publique peut jouer un rôle de « référence » sur les bonnes pratiques.**

Le point de vue de la puissance publique est d'inciter les organisations à adopter des règles identiques à celles imposées aux OIV (et à leurs sous-traitants) et aux « opérateurs essentiels » visés par la directive NIS.

L'un des premiers arrêtés sectoriels d'application de la LPM pour les OIV concerne le secteur de la santé. Tous les arrêtés sont construits sur la même trame et les dispositions sont réplicables. Cet arrêté définit des exigences : les règles de sécurité à appliquer, les types de systèmes d'information à déclarer à l'ANSSI et les types d'incidents de sécurité à notifier à l'ANSSI.

Concernant les données personnelles, le texte fait référence au GDPR européen (*General Data Protection Regulation* applicable au 25 mai 2018). Plus généralement, l'ensemble des normes de la famille ISO 270XX concourent à la mise en place de ces bonnes pratiques.

Un autre exemple « vertueux » dans le même domaine de la santé peut être trouvé dans l'Annexe au canevas de PSSI pour les structures des secteurs sanitaire et médico-social : Couverture des règles de la PSSIE (politique SSI de l'État) par les règles du canevas de PSSI[14].

Un espace dédié à la mise en œuvre des arrêtés LPM sur le site web de l'ANSSI établira le catalogue des références à utiliser : ce que les organisations doivent faire et les documents à disposition. Ce catalogue est orienté qualité et pilotage.

Le dispositif LPM s'inscrit dans le dispositif plus large de sécurité des activités d''importance vitale (SAIV), qui s'appuie sur des directives nationales de sécurité (DNS). Il introduit la notion de système d'information d'importance vitale (SIIV) : il s'agit des systèmes d'information les plus critiques des OIV, auxquels s'appliquent l'ensemble des obligations de la LPM.

---

[13] Jean-Laurent Santoni, *Le Ransomware est-il assurable ?*, revue Expertises voir http://www.expertises.info/droit-technologies-systemes-information/

[14] Voir http://www.esante.gouv.fr/en/pgssi-s/espace-publication

Les arrêtés sectoriels seront publics, mais certaines annexes (celles précisant les typologies d'attaques ainsi que les délais d'application des règles) ne seront pas publiées. La plupart des informations échangées entre les OIV et l'ANSSI dans le cadre de la mise en œuvre de ce dispositif seront protégées au niveau DR (Diffusion Restreinte), voire CD (Confidentiel Défense) si le besoin de confidentialité le justifie.

La gestion des incidents remontés à l'ANSSI dans le cadre de la LPM sera effectuée par le COSSI (centre opérationnel de la SSI). Un réseau sécurisé permettant l'échange d'informations DR entre l'ANSSI et les OIV sera mis en place courant 2017 pour faciliter ces échanges.

Quid de l'idée de groupement d'intérêt public (GIP) : un CERT national pour collecter l'information sur l'état de la menace, faire le lien avec les éditeurs, les entreprises et les utilisateurs ?

Recommandation

Des initiatives publiques tracent des pistes possibles.

- **Le projet de la plateforme d'assistance aux victimes de cyber malveillance**

La création de cette plateforme était annoncée dans la Stratégie Nationale pour la sécurité numérique[15] présentée 16 octobre 2015.

L'ANSSI va mettre en place, avec le ministère de l'Intérieur, une plateforme d'assistance aux victimes de cyber malveillance. La plateforme a vocation à assister toutes les victimes du particulier à la grande entreprise dès lors qu'elle n'est pas OIV (les OIV bénéficient d'ores et déjà de l'assistance de l'ANSSI en cas d'attaque). La plateforme permettra à la victime de rentrer en relation avec des prestataires ainsi qu'avec les services de police le cas échéant.

Son rôle éventuel, dans les assurances cyber, mérite un examen particulier. L'ANSSI et le MINT disposent de six à neuf mois pour définir la structure qui va porter ce projet et pour définir sa forme juridique. Un PPP est envisagé.

Cette plateforme a vocation à traiter les acteurs non OIV (PME et particuliers). C'est très différent de la LPM qui, elle, concerne justement les OIV, qui sont en lien direct avec l'ANSSI et notamment le COSSI pour la remontée d'incidents.

- **La qualification des acteurs – les experts de confiance**

Il s'agit d'inciter les entreprises à faire appel aux prestataires qualifiés (comme les experts dans l'immobilier) pour leurs besoins d'audit et de réponse à incident. Cela pourrait également s'appliquer aux produits qualifiés. La qualification repose sur deux piliers : la qualité/compétence et la confiance.

Le nombre de prestataires qualifiés ne sera pas suffisant pour couvrir l'ensemble des besoins d'expertises. Mais il semble important, sur des incidents cyber sensibles, que l'assureur et l'assuré puissent s'appuyer sur des experts de confiance. Le client doit pouvoir, par exemple, récuser une expertise qui puisse mettre en danger son activité. Ce droit d'opposition doit être contractuel.

Un métier nouveau serait à créer l' « Expert cyber tiers de confiance » comme une extension de la base PRIS (prestataire de réponse à incident de sécurité) qui est un label ANSSI.

- **Le dépôt de plainte – la mise sous scellés**

Ce sujet n'est pas simple. La judiciarisation et la mise sous scellés qu'elle provoque est préjudiciable pour la continuité des affaires. La crainte d'une mise sous scellé est un des verrous de la remontée d'incident. Cependant, il y a des obligations légales de dépôt de plainte qu'il s'agit de respecter. Le projet de loi pour une république numérique définit dans son article 20bis les nouvelles conditions d'intervention des agents publics assermentés.

Il s'agit de bien articuler le calendrier des opérations de remédiation de l'incident cyber avec les opérations d'investigation nécessaires à l'enquête. Une des difficultés consiste à assurer la continuité de l'activité alors

[15] http://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf

qu'elle peut être affectée par les besoins de l'enquête (saisie de preuves, interrogations des acteurs). Dans la rédaction et l'application des PCA/PRA (plans de continuité et de reprise d'activités après incidents), ces questions doivent être traitées.

Les nouvelles architectures « Cloud » ne facilitent évidemment pas la compréhension des attaques et leur attribution. Des clauses, dans les contrats d'assurance, devront traiter ces aspects en s'inspirant, par exemple, de celles concernant les vols où la plainte libère le mécanisme assurantiel.

La remontée d'incident vers la plateforme de l'ANSSI sera sans lien avec la judiciarisation de l'évènement. Les compétences de l'ANSSI ne sont pas judiciaires (particularité du dispositif français). Mais le projet est porté par l'ANSSI et le MINT. Ce point est à éclaircir.

- **Le Tiers de confiance pour le dialogue sur les incidents de cybersécurité entre assurés et assureurs**

Deux difficultés principales doivent être résolues :

  - Partager des données sensibles et probantes en toute sécurité entre l'assuré et l'assureur pour bien qualifier et quantifier le risque cyber ;
  - Disposer de données statistiques « anonymisées » et pertinentes pour le calcul des primes et le travail des actuaires.

Recommandations

Une solution possible consisterait à mettre en place une plateforme neutre d'échange d'information entre l'assureur et l'assuré.

Idée pour une plateforme

Etudier l'opportunité de mettre en place une plateforme neutre d'échange d'information entre l'assureur et l'assuré. Elle pourrait être opérée par un tiers de confiance à définir. Cette « Plateforme mutualiste sécurisée pour la maîtrise et l'assurance du risque cyber » pourrait être à but non commercial sous la forme d'un Partenariat Public Privé entre une émanation de l'ANSSI et les Compagnies d'assurance.

Le processus opérationnel de fonctionnement de cette plateforme doit faire l'objet d'une étude plus approfondie.

ANNEXE 1 - La lettre d'invitation

Madame, Monsieur,

Nous vous invitons à participer à une première table ronde fermée sur le thème de l'assurance du risque cyber dans sa dimension systémique.

Nous souhaitons réunir, dans le cadre plus large d'une réflexion relative à la « cybersécurité des systèmes du futur », des parties prenantes privées et publiques intéressées par la question du risque cyber et son assurance. Nous intégrons les points de vue du client industriel, de l'assureur ou réassureur et des organismes publics de régulation ainsi que ceux des représentants des associations professionnelles françaises et européennes.

La réflexion portera sur la problématique de la maîtrise du risque cyber sur l'ensemble de la chaîne de sa valeur et son transfert vers l'assurance à travers cinq séminaires fermés qui auront lui entre novembre 2015 et juin 2016. L'objectif étant de produire des propositions d'actions (livre blanc, recommandations législative ou réglementaire).

Il s'agira de recueillir les premiers éléments de réflexion afin de proposer un cadre de référence européen pour la gestion du risque cyber. L'objectif est d'arriver à un standard : qualifier l'incident du point de vue du client industriel et de l'assureur, des catégories communes et une méthodologie qui apporte aux organisations et aux assureurs et réassureurs un cadre sectoriel qui réponde aux exigences légales et techniques ; mais aussi au sens de la continuité des activités industrielles en cas d'attaque, la vision du secteur du cycle de l'indemnisation, le soutien au maintien et à la reprise d'activité. Sur l'ensemble de ces sujets, nous souhaitons bénéficier de vos avis et réflexions.

Nous nous adressons à vous sur recommandation des organismes et des personnes ayant déjà entamé des travaux que nous exploitons comme base d'analyse.

Ces réflexions s'inscrivent dans un projet de recherche finalisée EIC (Environnement pour l'Interopérabilité et l'Intégration en Cybersécurité) menée au sein de l'Institut de Recherche Technologique (IRT)-SystemX dont la vocation est de réunir des partenaires publics et privés intéressés pour mettre en œuvre le plan de développement de la filière cyber européenne. Les travaux sont financés paritairement par des industriels, notamment Airbus Group, et par le Secrétariat Général de la Défense et de la Sécurité Nationale/Agence Nationale de Sécurité des Systèmes d'Information. EIC a une finalité technique par le développement et la mise à disposition d'une plateforme de simulation d'attaques sur les systèmes du futur. Le projet dispose aussi d'une dimension économétrique et financière (modélisation du coût d'une attaque cyber et de la valorisation du circuit assurantiel) ainsi que d'une doctrine juridique conforme au modèle européen qui appuiera le développement économique de la filière numérique.

Les experts d'Airbus Group, M. Philippe Cotelle (Insurance and Risk Management), Mme Bénédicte Suzan (affectée à l'IRT-SystemX) avec l'appui de M. Philippe Wolf (directeur du programme EIC) sont chargés de monter et conduire les séminaires pour en exploiter les résultats. Ces échanges seront confidentiels.

Dans l'attente de vous rencontrer, je vous prie d'agréer, Madame/Monsieur, l'assurance de ma sincère considération.

Philippe WOLF

ANNEXE 2 – Participants

Nous avons consulté des organismes acteurs du sujet à travers des personnes qualifiées, recommandées et invitées à participer aux travaux de réflexion durant la première année de notre programme de recherche. Cette liste n'est pas exhaustive.

Assureurs :

- AXA Entreprise.

Réassureurs :

- SCOR ;
- Munich-Re France.

Courtiers :

- Clevercourtage ;
- Marsh.

Associations professionnelles :

- FERMA-AMRAE ;
- FFA ;
- CIGREF ;
- Institut des actuaires.

Cabinet d'avocats

- KGA.

Prévention des risques

- Bureau Véritas.

Industriels, PME

- Airbus Group ;
- MBDA ;
- Lineon.

Organisation internationale :

- OCDE (2 départements).

Ministère de l'Économie, de l'Industrie et du Numérique

- Direction générale des entreprises (DGE) ;
- Direction générale du Trésor, Sous-direction des Assurances ;
- Direction des affaires juridiques (DAJ) ;
- Conseil général de l'économie (CGE) : section Sécurité et Risques.

Ministère de la Défense

- Direction générale de l'armement (DGA-ITE).

SGDSN / ANSSI

IRT-SystemX

- directeur du programme EIC ;
- le chercheur en charge du domaine juridique.

ANNEXE 3 – Groupe de travail

Liste nominative des participants.

Alain Ribera	alain.ribera[at]airbus.com
Bénédicte Suzan	benedicte.suzan[at]irt-systemx.fr
Cécile Vignial	cecile.vignial[at]oecd.org
Christian Daviot	christian.daviot[at]ssi.gouv.fr
Christophe Delcamp	c.delcamp[at]ffsa.fr
David Crochemore	david.crochemore[at]ssi.gouv.fr
Didier Parsoire	dparsoire[at]scor.com
Elettra Ronchi	elettra.ronchi[at]oecd.org
Elisabeth Rolin	elisabeth.rolin[at]ssi.gouv.fr
Florence Picard	florencepicard[at]aol.com
François Beaume	francois.beaume[at]bureauveritas.com
Françoise Roure	francoise.roure[at]finances.gouv.fr
Gilbert Canameras	gilbert.canameras[at]erametgroup.com
Gilbert Flepp	gilbert.flepp[at]acegroup.com
Isabelle Hirayama	isabelle.hirayama[at]irt-systemx.fr
Jean-François Pepin	jean-francois.pepin[at]cigref.fr
Jean-Laurent Santoni	jean-laurent.santoni[at]clevercourtage.com
Jean-Paul Defransure	jean-paul.defransure[at]mbda-systems.com
Laurent Bernat	laurent.bernat[at]oecd.org
Laurent Celerier	laurent.celerier[at]ssi.gouv.fr
Luc Vignancour	luc.vignancour[at]marsh.com
Laurent-Xavier Simonel	lx.simonel[at]kga.fr
Nathalie Convert	n.convert[at]ffsa.fr
Olivier Allaire	olivier.allaire[at]lineon.fr
Philippe WOLF	philippe.wolf[at]irt-systemx.fr
Philippe Cotelle	philippe.cotelle[at]airbus.com
Philippe Gaillard	philippe.gaillard[at]axa.fr

Philippe Laflandre	philippe.laflandre[at]airbus.com
Patrick Pouillot	ppouillot[at]munichre.com
Sébastien Heon	sheon[at]scor.com
Shirley Plumerand	shirley.plumerand[at]gmail.com
Stanislas Chapron	stanislas.chapron[at]marsh.com
Stéphane Spalacci	s.spalacci[at]ffsa.fr
Vincent Desroches	vincent.desroches[at]ssi.gouv.fr

ANNEXE 4 – L'IRT-SystemX

Labellisé le 1er février 2012, l'IRT-SystemX achève sa première phase triennale en ayant développé une expertise et un socle technologique unique via 17 projets de recherche colocalisant sur son site, 61 partenaires industriels et 14 académiques. Pour 2016-2020, l'objectif est de développer 4 grands programmes de recherche (ingénierie systèmes, transport autonome, territoires intelligents, internet de confiance), étendre l'usage des 7 plateformes créées en son sein et accroître son rayonnement à l'international. L'IRT-SystemX bénéficie du statut de fondation pour la coopération scientifique et des leviers des investissements d'avenir.

L'ambition est de développer des applications orientées marché et usages pour aider les industriels dans la transformation numérique de leur entreprise et leurs produits. Donc de répondre aux défis que rencontrent les industriels dans les phases de conception, de modélisation, de simulation et d'expérimentation des innovations futures qui intègrent de plus en plus de numérique au travers de quatre programmes :

- L'ingénierie systèmes : Développer des méthodes, des processus et des outils logiciels d'ingénierie collaborative pour les systèmes complexes, dans le contexte de l'entreprise étendue, tout en s'appuyant sur le potentiel des technologies numériques.
- Le transport autonome : Développer de nouvelles architectures sécurisées et sûres pour les véhicules et systèmes de transport autonomes, intégrant les nouveaux usages, les systèmes embarqués critiques, l'évolution des infrastructures et leurs interactions.
- L'Internet de confiance : Développer les algorithmes, les protocoles et les architectures sur lesquels reposeront les infrastructures numériques de demain, socle de la transformation numérique.
- Les territoires intelligents : Développer des outils d'aide à la décision pour l'optimisation et la planification opérationnelle de l'évolution des territoires, en s'appuyant sur la collecte et l'analyse des données.

Le fonctionnement de l'institut repose sur deux aspects fondamentaux :

- la colocalisation de ses talents ;
- la mutualisation des compétences et des plateformes.

Une convention entre l'IRT-SystemX, l'ANSSI et Airbus Group couvre des actions de recherche en relation avec la protection et la défense des systèmes d'information. Ces travaux concernent les interactions entre les hommes et les techniques en cybersécurité dans leurs dimensions économiques et réglementaires. Ils visent à promouvoir les usages de confiance dans l'environnement numérique.

Les travaux de recherche de l'IRT sont validés par l'ANR (l'Agence nationale pour la recherche).

ANNEXE 5 – Le projet EIC

EIC : Environnement pour l'Interopérabilité et l'Intégration en Cybersécurité. Début des travaux, le 2 février 2015. Le programme de recherche est établi pour 5 ans. Le montant global du projet de recherche est estimé à 10M€, 12 ETP (montée en puissance prévue), 6 partenaires industriels à ce jour (Airbus Group, Bertin, Engie, Gemalto, Prove&Run, Thalès), des partenaires académiques (UTT de Troyes, IMT – Mines Télécom et CEA).

La protection des systèmes d'information et des données qu'ils véhiculent nécessite des arbitrages complexes entre la facilité d'usage, le coût de la sécurité, de la sûreté de fonctionnement et du respect d'un droit numérique en évolution constante afin d'offrir les conditions nécessaires à leur déploiement sur un marché ouvert pour créer rapidement de la valeur et réunir les conditions de la prospérité économique.

Plateforme CHESS : Cybersecurity Hardening Environment for Systems of Systems sur un financement de l'ANSSI à hauteur de1M€ sur 5 ans.

Dans ses 4 premières taches de recherche appliquée, le projet EIC met en œuvre la plateforme CHESS expérimentale et technique cyber afin évaluer le couplage de technologies de cybersécurité à travers des cas d'usage innovants dans le domaine des SmartGrids, de l'Usine du Futur, du Transport Connecté et Autonome et des nouveaux services de l'Internet des Objets.

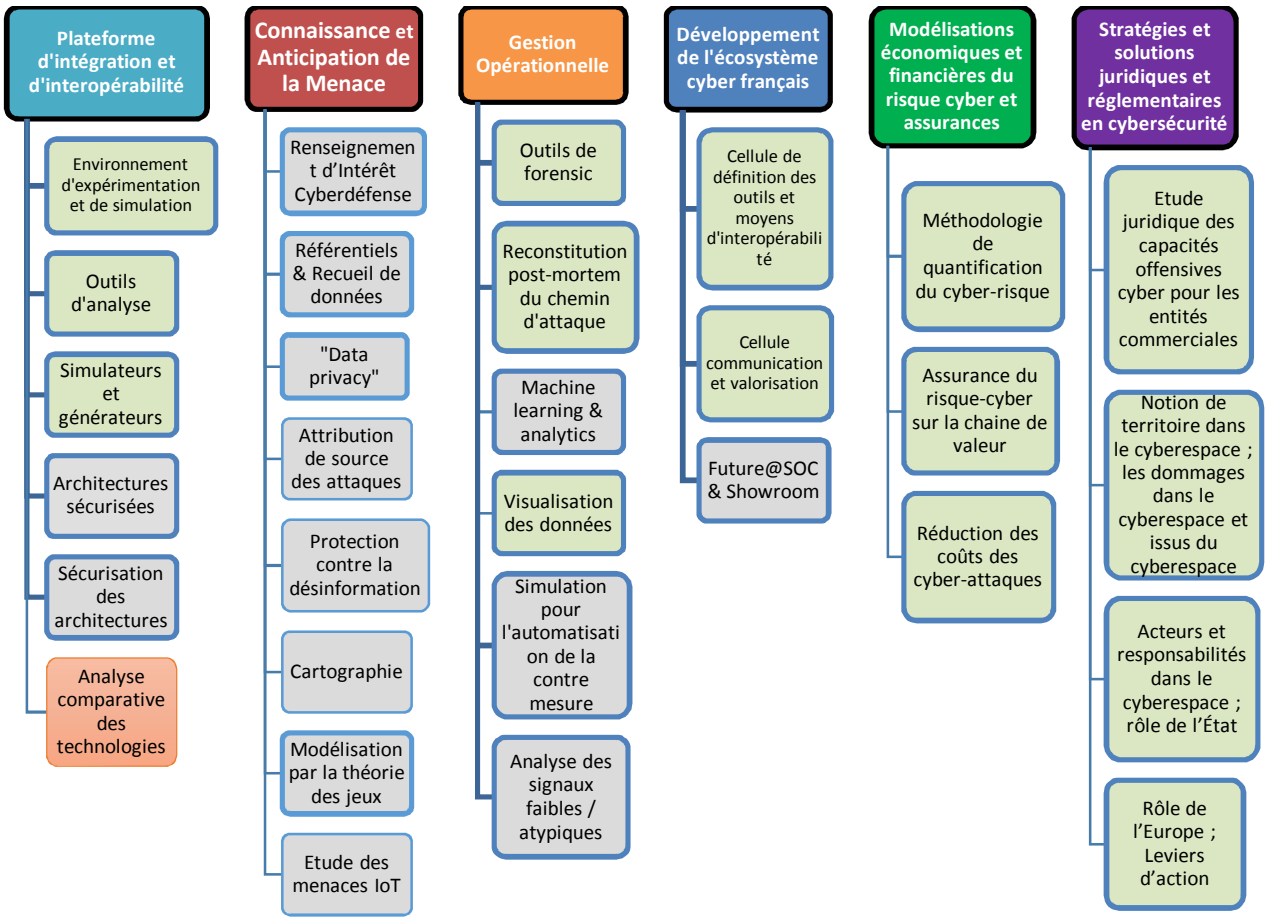


Figure 7 : décomposition du programme de recherche EIC en tâches et sous-tâches

Airbus Group finance depuis le 1er septembre 2015, les tâches 5 et 6 d'EIC qui viennent en appui des tâches 1 à 4 pour accompagner le développement des cas d'usage et permettre l'insertion de ces nouvelles technologies après leur développement sur le marché. L'ANSSI finance également et, est directement partie prenante dans la définition des thèmes et la conduite de la recherche. Le financement de T5 et de T6 est ouvert à d'autres partenaires privés.

T5 et T6 traitent conjointement et de façon cohérente avec tâches 1 à 4 d'EIC des composantes économique/économétrique, financière, assurantielle et juridique du risque cyber.

Ces deux thèmes de recherche sont menés dans le cadre d'un Partenariat Public Privé faisant également appel à des acteurs extérieurs dont les compétences et la validation sont nécessaires et indispensables a priori.

T5.1 produit des travaux novateurs de modélisation économétrique afin de proposer une quantification du risque cyber et un mode de représentation afin de permettre aux responsables et au management de prioriser les investissements cyber et ensuite de réduire le risque (mitiger).

T5.2 traite des conditions nécessaires pour connaître, gérer et maitriser le risque cyber pour ensuite le transférer vers l'assurance. L'objectif étant de lever les verrous qui freinent aujourd'hui la compréhension risque cyber au sein des organisations et celles qui bloquent le développement du marché assurantiel de la cybersécurité. L'objectif de T5.2 est de pointer les obstacles et de produire des recommandations pour les lever dans un temps court au travers d'un plan d'action en fonction des calendriers législatifs et réglementaires en cours (nationaux et internationaux).

Les travaux juridiques et réglementaires de T6 permettent à EIC d'introduire la sécurité juridique by design afin que les produits de la recherche appliquée et de l'innovation soient directement et dès le début encadrés et promus par un droit efficace pour les industriels sur le marché intérieur européen, mais aussi à l'extérieur (créateur de richesse et de croissance).

Les travaux d'intelligence juridique et stratégiques s'appuient sur une analyse pratique du droit et de la stratégie des Etats et industriels qui concourent ensemble via l'IRT-SystemX, à l'élaboration du droit « cyber » par les Etats-Unis, afin d'en extraire la meilleure stratégie nationale pour ce secteur et les arguments légaux à même de conforter la position des industriels européens émergente.

Les outils et les méthodes de T6 viendront en appui à T5.2 (gestion du risque cyber/assurance) en apportant une expertise quant à l'évaluation juridique du risque cyber pour les industriels, les assureurs et réassureurs, l'Etat et les autorités de contrôle. Il s'agit d'analyser les éléments fondamentaux et du partage des responsabilités pour une assurance cyber en adéquation avec les industriels et les objectifs poursuivis par la stratégie nationale pour la sécurité du numérique.

La production de T6 doit être insérée dans une chaîne de contrôle et de la validation des avis et des recommandations qu'il élabore. Les travaux juridiques seront en effet conduits en lien étroit avec la direction juridique du SGDSN/ANSSI. Les résultats de la recherche de T5.2 pourront être ainsi être portés par l'ANSSI, service à compétence nationale, en capacité de produire des règlements, porter des propositions de loi vers l'Assemblée nationale, les instances de l'Union européenne (ENISA G29) et les organisations internationales telles que l'ONU, OCDE.

ANNEXE 6 - Bibliographie

Cette bibliographie couvre les principaux documents exploités lors de nos travaux. Elle ne peut être exhaustive sur un sujet aussi vaste.

France

1. Denis Kessler, *Les sociétés modernes face aux risques extrêmes*, Risques n°76, décembre 2008.
2. L'AMRAE nous a transmis une documentation décrivant un « Outil d'aide à l'analyse et au traitement assurantiel des cyber risques » réalisé en partenariat avec le CESIN. La méthode est disponible ici : http://www.cesin.fr/publications/document/download/20
3. Stéphane LIPSKI, Quantification du risque et du sinistre indemnisable : point de vue de l'expert, AFDIT, 14/04/2014, http://www.afdit.fr/media/pdf/3%20avril%202014/Probl%C3%A9matiques%20Juridiques.pdf
4. Jean-Laurent SANTONI, Loi de programmation militaire Contribution de l'assurance des cyber risques, Expertises - Avril 2014, http://www.cyberisques.com/fr/mots-cles-40-financement-cyber-risque/244-idees-jean-laurent-santoni-clever-courtage
5. Panorama d'actualités du droit de l'économie numérique, Paris 4 Juin 2015, AFDIT
6. Compagnie Nationale des Experts de Justice en Informatique et Techniques Associées, L'évaluation des préjudices dans le monde numérique, Les liens de causalité au cœur de la démonstration, Colloque du 9 avril 2013, http://www.lagbd.org/images/1/11/Colloque_CNEJITA_L'%C3%A9valuation_des_pr%C3%A9judices_dans_le_monde_num%C3%A9rique.pdf
7. FFSA, Panorama de la cyber-assurance, Conférence AMIECE du 30 novembre 2015, http://www.amiece.org/IMG/pdf/151130_AMIECE_-_Panorama_de_la_cyber-assurance.pdf
8. Grégoire Loiseau, Matthieu Bourgeois, *Du robot en droit à un droit des robots*, La Semaine Juridique, 24 Novembre 2014, Hebdomadaire n°48.
9. Alizée LETROSNE, Le droit des robots, Mémoire sous la direction de M. le Professeur William GILLES, 10 juin 2015, Université Paris 1 Panthéon Sorbonne.
10. Jean-Laurent SANTONI, *Risques et assurances, Assurabilité des conséquences pécuniaires des cyber risques*, Expertises - Avril 2013.
11. Claire BERNIER, Jean-Laurent SANTONI, *L'assurance comme moyen d'indemnisation des nouveaux risques numériques de l'entreprise, Journal des Sociétés*, n°127 Février 2015, http://www.clevercourtage.com/wp-content/uploads/2015/03/JSS-Lassurance-comme-moyen-dindemnis-ation-C.-Bernier-JL-Santoni.pdf
12. *L'APPLICATION DU PRINCIPE NE BIS IN IDEM DANS LA RÉPRESSION DES ABUS DE MARCHÉ Proposition de réforme*, AMF Mai 2015, http://www.amf-france.org/technique/multimedia?docId=workspace://SpacesStore/7cb9fffa-2fc6-45ad-babc-aee62d3f2a17_fr_1.0_rendition
13. ANSSI, *Référentiel de qualification de prestataires de services sécurisés d'informatique en nuage (cloud computing) - référentiel d'exigences*, Version 1.3 du 30/07/2014, http://www.ssi.gouv.fr/uploads/IMG/pdf/cloud_referentiel_exigences_anssi.pdf
14. Bernard Spitz, *L'assurance face au cyberrisque*, Les échos, 27/10/2015.

15. APREF (Association des Professionnels de la Réassurance en France), *Étude sur les « cyber-risques » et leur (ré)assurabilité*, Juin 2016.

16. René-François BERNARD, Ilarion PAVEL, Henri SERRES, Rapport à Monsieur le Ministre de l'Économie, de l'Industrie et du Numérique, *Cyberassurance*, 20 avril 2015.

17. Thèse professionnelle rédigée par Julien Ménissez, Les cyber-assurances - Quels critères de décisions ?, Exécutive Mastère Spécialisé Management Stratégique de l'information et des Technologies, HEC Paris – MINES ParisTech, 2015.

18. FFSA, *Cyber-Risques et Protection des données personnelles*, 27 juin 2016.

19. Banque de France, *Évaluation des Risques du Système financier Français*, Décembre 2015, https://www.banque-france.fr/fileadmin/user_upload/acp/publications/ERS-001-20150715.pdf

20. Philippe Wolf, *Some considerations about privacy*, http://www.irt-systemx.fr/v2/wp-content/uploads/2015/11/privacy-pw-irt-systemx.pdf

21. Isabelle Hirayama, Bénédicte Suzan, Philippe Wolf, *Active and Proactive Defence in Cyberspace*, IRT-SystemX, 10 juin 2016.

22. Arrêté du 10 juin 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Produits de santé » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032749532&dateTexte=&categorieLien=id

23. Arrêté du 17 juin 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au secteur d'activités d'importance vitale « Gestion de l'eau » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032749580&dateTexte=&categorieLien=id

24. Arrêté du 17 juin 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au secteur d'activités d'importance vitale « Alimentation » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032749626&dateTexte=&categorieLien=id

25. Code des assurances, 1er janvier 2016, http://www.cjoint.com/doc/16_01/FAioYVSo2cb_codedesassurances2016.pdf

UE

26. European Data Protection Supervisor, *Report Survey 2015, Measuring compliance with data protection rules in EU institutions*, 21 January 2016, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2016/16-01-21_Report_Survey_2015_EN.pdf

27. IAIS, *Global Insurance Market Report* (GIMAR) 2015, http://www.iaisweb.org/file/58465/2015-global

28. ENISA, *Big Data Threat Landscape and Good Practice Guide*, January 2016, https://www.enisa.europa.eu/publications/bigdata-threat-landscape/at_download/fullReport

29. DIRECTIVE 2009/138/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009 on the *taking-up and pursuit of the business of Insurance and Reinsurance* (Solvency II), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:335:0001:0155:en:PDF

30. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE) http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679

31. Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil

32. Marsh, *European 2015 Cyber Risk Survey Report*, https://www.marsh.com/uk/insights/research/european-2015-cyber-survey-report.html

33. ENISA, *ENISA Threat Landscape 2015*, https://www.enisa.europa.eu/publications/etl2015/at_download/fullReport

34. ENISA, *Threat taxonomy*, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/threat-taxonomy-2015/at_download/file

GB

35. HM Government, *Cyber Essentials Scheme: Assurance Framework*, January 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400914/bis-15-72-cyber-essentials-scheme-assurance-framework.pdf

36. Cambridge Centre for Risk Studies, Cambridge Risk Framework, Cyber Catastrophe: Stress Test Scenario, *SYBIL LOGIC BOMB CYBER CATASTROPHE SCENARIO*, June 2014, https://www.researchgate.net/profile/Scott_Kelly2/publication/263262710_Stress_Test_Scenario_Sybil_Logic_Bomb_Cyber_Catastrophe/links/0046353a45b383dfc8000000.pdf?inViewer=0&pdfJsDownload=0&origin=publication_detail

37. Cambridge Center for Risk Studies, Cambridge Risk Framework, *Cyber Accumulation Risk Management*, February 2016, http://cambridgeriskframework.com/getdocument/39

38. COI-TENANT-INSURANCE-REQUIREMENTS-2015, *LEASE AGREEMENT INSURANCE AND INDEMNIFICATION LANGUAGE*, http://230fifthave.com/wp-content/uploads/2015/08/COI-TENANT-INSURANCE-REQUIREMENTS-July-30-2015.pdf

39. Lloyd's *City Risk Index 2015-2025*, http://www.lloyds.com/cityriskindex/
Synthèse,
https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/city%20risk%20index/city%20risk%20exec%20summary_french.pdf

40. HM Government & Marsh, UK CYBER SECURITY, *THE ROLE OF INSURANCE IN MANAGING AND MITIGATING THE RISK*, March 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf

Suisse

41. Zurich Insurance Group, *Zurich identifies seven cyber risks that threaten systemic shock*, https://www.zurich.com/en/media/news-releases/2014/2014-0422-01

42. Global Center for Digital Business Transformation, *Digital Vortex How Digital Disruption Is Redefining Industries*, June 2015, http://www.imd.org/uupload/IMD.WebSite/DBT/Digital_Vortex_06182015.pdf

43. Zurich Insurance Group, *Risk Nexus Beyond data breaches: global interconnections of cyber risk*, April 2014, https://www.files.ethz.ch/isn/182163/Zurich_Cyber_Risk_April_2014.pdf

USA

44. Ponemon Institute LLC, 2015 and 2016 Cost of Data Breach Study: Global Analysis, May 2015 et 2016 https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF https://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03094wwen/SEL03094WWEN.PDF

45. Internet Security Alliance (ISA) / American National Standards Institute (ANSI), The Financial Management of Cyber Risk, 2010, http://www.isaca.org/chapters2/New-York-Metropolitan/membership/Documents/2011-12-15%20Adams%204.pdf

46. US Senate, Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security, Hearing entitled "Examining the Evolving Cyber Insurance Marketplace.", Thursday, March 19, 2015, Written Testimony of Michael Menapace, https://www.hsdl.org/?view&did=765042

47. Senate Committee on Commerce, Science, and Transportation, March 19, 2015, Hearing "*Examining the Evolving Cyber Insurance Marketplace*", Testimony of Ben Beeson, Vice President, Cyber Security and Privacy, Lockton Companies, Ola Sage, Founder and CEO e-Management and Catherine Mulligan, SVP Zurich, https://www.hsdl.org/?view&did=765042

48. The Betterley Report, Cyber/Privacy Insurance Markey Survey, June 2016, https://www.irmi.com/online/betterley-report-free/cyber-privacy-media-liability-summary.pdf

OCDE

49. OCDE, Instruments Juridiques sur les Politiques de l'Économie Numérique, 2015, *Gestion du Risque de Sécurité Numérique pour la Prospérité Économique et Sociale*, https://www.oecd.org/fr/sti/ieconomie/DSRM_French_final_Web.pdf

Divers

50. Institut canadian des actuaires, Research Paper on Operational Risk, November 2014, http://www.cia-ica.ca/docs/default-source/2014/214118e.pdf

51. Airmic, *Review of Recent Developments in the Cyber Insurance Market*, https://www.scor.com/fr/sgrc/vie/risques-psychosociaux/item/1716.html?lout=sgrc

52. Garifova L.F., *Infonomics and The Value of Information in The Digital Economy*, 2nd GLOBAL CONFERENCE on BUSINESS, ECONOMICS, MANAGEMENT and TOURISM, 30-31 October 2014, Prague, Czech Republic, http://isiarticles.com/bundles/Article/pre/pdf/52169.pdf

53. Doug Laney , Infonomics: *The Economics of Information and Principles of Information Asset Management*, The Fifth MIT Information Quality Industry Symposium, July 13-15, 2011, http://mitiq.mit.edu/IQIS/Documents/CDOIQS_201177/Papers/05_01_7A-1_Laney.pdf

54. Ranjan Pal, Pan Hui, CyberInsurance for CyberSecurity, A Topological Take On Modulating Insurance Premiums, http://www.deutsche-telekom-laboratories.de/~panhui/publications/insrRP.pdf

55. PartnerRe, *CYBER LIABILITY INSURANCE, MARKET TRENDS: SURVEY*, October 2015, http://www.partnerre.com/assets/uploads/docs/PartnerRe_Cyber_Liability_Trends_Survey_2015.pdf

56. Institute of Insurance Economics, University of At. Gallen, INSURABILITY OF CYBER RISK: AN EMPIRICAL ANALYSIS, January 2015, http://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/wps/wp151.pdf

57. InfoCyndinique, http://ifrei.org/tiki-index.php?page=InfoCindynique

58. Nassim Nicholas Taleb, *Silent Risk*, https://drive.google.com/file/d/0B8nhAlfIk3QIR1o1dnk5ZmRaaGs/view?pref=2&pli=1

ANNEXE 7 – Glossaire

Il s'agit d'un travail préliminaire qui devra être consolidé. En aucun cas cela n'engage le marché de l'assurance.

ASSURÉ

Personne qui est garantie par un contrat d'assurance. [Larousse]

ASSUREUR

Personne qui s'engage, moyennant le paiement d'une prime ou d'une cotisation, à payer à l'assuré ou au bénéficiaire désigné un capital ou une rente en cas de survenance d'un risque déterminé. [Larousse]

ATTEINTE AUX DONNÉES

En droit de l'informatique, ce que l'on nomme communément le piratage relève des atteintes aux systèmes de traitement automatisé de données (STAD). Issues initialement de la loi dite « Godfrain » ces infractions se retrouvent principalement sous les articles 323-1 à 323-7 du code pénal.

La définition ci-après n'est pas consolidée.

1. Toute altération, destruction, suppression, corruption, inutilisation, illisibilité, inaccessibilité, impossibilité de traitement des ***données***, résultant :

- de tout acte commis par un ***préposé*** de l'***assuré*** ou par un ***tiers*** visant à accéder ou se maintenir frauduleusement, dans tout ou partie du ***système d'information*** de l'***assuré*** ou à entraver ou fausser le fonctionnement du ***système d'information*** de l'***assuré,***
- d'une attaque en ***déni de service***,
- de la réception ou la transmission d'un ***code ou logiciel malveillant***,
- d'un incident technique affectant le système d'information de l'assuré,
- d'un dommage matériel affectant le système d'information de l'assuré,
- d'une erreur humaine ou erreur de programmation,
- d'une interruption non intentionnelle et imprévue du ***système d'information*** de l'***assuré.***

2. Toute divulgation ou transmission sans autorisation de ***données.***

3. Toute soustraction frauduleuse de ***données.***

4. Toute violation de la ***norme PCI DSS.***

CODE OU LOGICIEL MALVEILLANT

Programme ou application, notamment virus, logiciel espion, vers informatique cheval de Troie, ransomware, keyloggers, …, conçu aux fins d'accéder ou de se maintenir frauduleusement au sein du ***système d'information***,

d'en surveiller, entraver ou fausser le fonctionnement ou d'introduire, altérer ou détruire des informations qu'il renferme. [ANSSI[16]]

CONSÉQUENCES PÉCUNIAIRES DE LA RESPONSABILITÉ CIVILE

Mise en jeu de la Responsabilité civile de l'assuré pour couvrir les dépenses nécessaires à l'indemnisation des préjudices subis par des tiers lorsque l'assuré en est civilement responsable. Ces préjudices sont :

- Dommages corporels subis par les tiers : un dommage portant atteinte à l'intégrité physique d'une personne autre que l'assuré (blessures, invalidité ou décès
- Dommages matériels subis par les tiers : toute détérioration ou destruction totale ou partielle d'un bien matériel appartenant à un tiers.
- Dommage immatériel : « tous dommages autres que corporels ou matériels » c'est-à-dire soit la réparation des dommages moraux (préjudices extrapatrimoniaux telles que les atteintes à la réputation, à la considération…), soit la réparation de dommages pécuniaires.

Les assureurs, dans leur définition des dommages immatériels, mettent généralement l'accent sur les dommages pécuniaires : « tout préjudice pécuniaire résultant de la privation de jouissance d'un droit, de l'interruption d'un service rendu par une personne ou par un bien ou de la perte d'un bénéfice ». Il s'agit de réparer le gain manqué par le tiers. On distingue :

- Dommages immatériels consécutifs à un dommage garanti: Dommage pécuniaire subi par le tiers victime et qui est la conséquence directe d'un dommage matériel ou corporel garanti par le contrat RC de l'assuré.
- Dommages immatériels consécutifs à un dommage non garanti : Dommage pécuniaire, subi par le tiers victime, qui n'est pas la conséquence d'un dommage matériel ou corporel garanti par le contrat RC de l'assuré.

Le tiers subit un dommage corporel ou matériel mais ce dommage n'est pas garanti par le contrat RC souscrit par l'assuré. Seules les conséquences pécuniaires (manque à gagner) de ce dommage initial sont garanties. Le dommage initial doit être susceptible de mettre en jeu la responsabilité de l'assuré (ex : vices cachées).

[définitions issues des conventions spéciales incendie de l'APSAD (Assemblée Plénière des Sociétés d'Assurances Dommages), 1982. Elles peuvent varier d'un assureur à l'autre]

CYBER-EXTORSION

[non consolidé]

Toute action ou menace d'action sur les ***données*** ou sur le ***système d'information*** de l'***assuré*** dans le but d'obtenir une rançon.

La forme la plus répandue de cyber-extorsion consiste à demander une rançon contre la remise d'une clé permettant le décryptage des données[17].

[16] Le glossaire de l'ANSSI définit l'ensemble des termes techniques relevant de la SSI, voir http://www.ssi.gouv.fr/entreprise/glossaire/

[17] Voir http://cyber-serenite.fr/cyber-lexique

CYBERSÉCURITÉ

État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre **la disponibilité, l'intégrité ou la confidentialité** des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense. [ANSSI]

CYBER-TERRORISME

Dans le droit français, le terrorisme est « une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur ».

Toute action ou menace de destruction, dégradation, modification ou perturbation (y compris ***déni de service***) des ***données*** et/ou du ***système d'information*** de l'***assuré*** dans le but de causer des dommages et/ou d'intimider toute personne pour des raisons sociales, idéologiques, religieuses, politiques ou tout objectif similaire. [non consolidé]

DÉNI DE SERVICE

Action ayant pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu. [ANSSI]

Privation totale ou partielle d'origine malveillante du service des ***systèmes d'information*** de l'***assuré*** sans que les équipements informatiques, les équipements de télécommunication ou les installations d'infrastructure de l'***assuré*** subissent un ***dommage matériel*** ou une destruction. [non consolidé]

DOMMAGE CORPOREL

Un dommage portant atteinte à l'intégrité physique d'une personne [APSAD].

DOMMAGE MATÉRIEL

Toute détérioration d'un bien meuble ou immeuble, toute atteinte physique à des animaux [APSAD].

DOMMAGE IMMATÉRIEL

Tous dommages autres que corporels ou matériels. C'est-à-dire soit la réparation des dommages moraux (préjudices extrapatrimoniaux telles que les atteintes à la réputation, à la considération…), soit la réparation de dommages pécuniaires [APSAD].

DONNÉE

Représentation conventionnelle d'une information en vue de son traitement informatique [Larousse].

Toute information échangée, traitée et/ou stockée sous format électronique et/ou tout média digital, notamment les ***données personnelles*** et les ***données confidentielles,*** les logiciels et les supports de ***données***. [non consolidé]

DONNÉES CONFIDENTIELLES

Toute information confidentielle appartenant ou confiée à l'***assuré***, tels que les procédures, les documents, les dessins, les formules ou les informations protégées par un secret professionnel institué par la loi, les règlements, les usages ou qui ne sont pas dans le domaine public. [non consolidé]

DONNÉES PERSONNELLES

Donnée à caractère personnel : « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne » [Art. 2 loi I&L].

Toute information identifiant ou permettant d'identifier une personne physique par référence notamment à un numéro, un nom, un mot de passe, des éléments ou critères qui lui sont propres (y compris les données médicales), appartenant ou confiée à l'***assuré***. [non consolidé]

ERREUR HUMAINE

Toute négligence ou erreur commise par un ***préposé*** de l'***assuré*** ou par un prestataire externe dans le cadre de l'exploitation, la maintenance et la mise à jour du ***système d'information***. [non consolidé]

ERREUR DE PROGRAMMATION

Toute erreur de conception, de développement ou d'encodage d'un logiciel, d'une application, d'un système d'exploitation ou d'un micro-code. [non consolidé]

FAIT DOMMAGEABLE

Le ***fait dommageable*** est celui qui constitue la cause génératrice du dommage ; un ensemble de ***faits dommageables*** ayant la même cause technique est assimilé à un ***fait dommageable*** unique. [non consolidé]

FAUTE PROFESSIONNELLE

Toute faute ou tout acte fautif, tout manquement, toute négligence ou omission, toute déclaration inexacte ou trompeuse, toute infraction aux dispositions légales, réglementaires ou statutaires, commise dans le cadre des activités de l'***assuré***. [non consolidé]

FRAIS DE COMMUNICATION ET DE NOTIFICATION

Frais liés à une violation de l'obligation de protection des données personnelles : dépenses engagées par l'assuré pour se conformer à ses obligations légales ou règlementaires à la suite d'une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données personnelles, ou l'accès non autorisé à de telles données.

Cette garantie porte sur :

- \- Les frais de notification aux instances administratives (CNIL, Premier ministre et ANSSI)
- \- Les frais de comparution (enquêtes administratives)
- \- Les frais de notification aux personnes concernées par la violation de ses données à caractère personnel [APSAD].

FRAIS DE DÉFENSE

Les honoraires et frais engagés par l'***assuré*** pour les besoins de sa défense, notamment :

- -les frais d'avocats,
- -les frais d'expertise,

- -les frais de procédure et de comparution. [non consolidé]

FRAIS DE MONITORING ET SURVEILLANCE

Frais engagés par l'***assuré*** avec l'accord préalable de l'***assureur*** pour détecter et contrôler en cas d'***atteinte aux données*** toute éventuelle utilisation inappropriée. [non consolidé]

FRAIS DE RESTAURATION

Les frais engagés par l'***assuré*** pour déterminer si les ***données*** peuvent ou non être restaurées ou reconstituées, pour décontaminer, nettoyer, restaurer, reconstituer les ***données*** et leur support.

Les frais d'adaptation, de reconfiguration de logiciels, le coût d'acquisition des licences de remplacement.

Le coût d'initialisation des systèmes de contrôle d'accès. [non consolidé]

FRAIS DE RESTAURATION D'IMAGE

Frais liés au rétablissement de l'E-réputation et à la communication : dépenses engagées pour rétablir la réputation/l'image de l'assuré auprès du public.

Sont compris, les frais de :

- Conseil en communication / relations publiques / Gestion de crise : frais liés aux conseils délivrés par des professionnels de la communication et de la gestion de crise.
- Nettoyage / noyage : technique consistant à développer sa présence sur le web (et donc sur les moteurs de recherche) dans le but de faire reculer les résultats gênants dans les toutes dernières pages de résultats. Pour que les informations négatives concernant l'entreprise visée soient les moins visibles possible des internautes, les informations négatives vont être noyées en créant de nombreux contenus.
- Frais de re-référencement : frais destinés à payer des informaticiens ou acheter un logiciel pour faire en sorte que le site web de l'entreprise soit à nouveau visible et en première page dans les moteurs de recherche.
- Plateforme téléphonique : Frais liés à la mise en place de frais de téléphonie supplémentaire afin d'informer et/ou de répondre à la clientèle [APSAD].

FRAIS ET PERTES CONSÉCUTIFS A LA VIOLATION DE LA NORME PCI DSS (Payment Card Industry - Data Security Standard)

Les frais engagés et pertes supportées par l'***assuré*** résultant de la violation par l'***assuré*** de la ***norme PCI DSS***, dont :

- Les honoraires d'expert mandaté en vue d'identifier l'origine de la violation de la ***norme PCI DSS***,
- Les pénalités contractuelles imposées à l'***assuré***,
- Les frais engagés en vue de l'obtention du renouvellement de la certification aux ***normes PCI DSS***,
- Les frais de réémission des cartes bancaires. [non consolidé]

FRAIS LIÉS A UNE MENACE DE CYBER-EXTORSION

Dommage pécuniaire : pertes de fonds ou de valeurs monétaires consécutives à des agissements à caractère délictueux tels que des escroqueries, extorsions, chantages, abus de confiance ou de biens sociaux.

Il s'agit d'obtenir de l'assureur :

- Le remboursement des fonds détournés, des rançons ou des sommes extorquées
- La prise en charge des frais de recours et de poursuite contre l'auteur du délit

Attention : la notion d'actifs financiers peut, là encore, prêter à confusion dans la mesure où ce terme désigne tout titre ou contrat, généralement transmissible et négociable sur un marché financier, qui est susceptible de produire à son détenteur des revenus ou un gain en capital, en contrepartie d'une certaine prise de risque. La notion est donc inappropriée pour l'assurance, il serait préférable de lui substituer celle de dommages pécuniaires puisqu'il s'agit de faire état d'une perte de fonds pour l'entreprise, d'une atteinte à sa trésorerie, consécutive à une infraction pénale appauvrissant le patrimoine de la victime [APSAD].

FRAIS SUPPLÉMENTAIRES D'EXPLOITATION

Les frais exposés par l'***assuré*** afin de limiter la durée d'interruption du ***système d'information***. [non consolidé]

FRANCHISE

Clause d'une assurance qui fixe un montant restant à la charge de l'assuré en cas de dommage ; ce montant lui-même. [Larousse]

INCIDENT TECHNIQUE

Défaillance ou panne mécanique des composants critiques du ***système d'information*** de l'***assuré*** qui détruit, altère, rend illisible ou inaccessible les ***données*** et résultant notamment des évènements suivants :

- Surcharge électrostatique ou perturbations électromagnétiques
- Surchauffe
- Action de l'électricité ou de la foudre [non consolidé]

MONTANT DE LA GARANTIE

Le montant maximal d'indemnisation, y compris les ***frais de défense***, par ***sinistre*** et par ***période d'assurance***. [non consolidé]

NORME PCI DSS

Norme publiée de sécurité des données (DSS) pour l'industrie des cartes de paiement (PCI).

PÉRIODE D'ASSURANCE

La période comprise entre :

- la date d'effet du contrat et la première échéance principale,
- deux échéances principales, sans pouvoir être supérieure à 12 mois consécutifs,
- la dernière échéance principale et la date de cessation des garanties. [non consolidé]

PRÉPOSÉ

Toute personne physique salariée ou non de l'***assuré***, agissant sous la direction, les ordres et la surveillance de l'***assuré***, y compris les stagiaires rémunérés ou non, les apprentis, les auxiliaires de vacances, le personnel intérimaire, le personnel détaché.

Par dérogation à ce qui précède, toute société ou toute personne externe à l'entreprise de l'***assuré*** mandatée par l'***assuré*** pour fournir des services informatiques, étant précisé que l'***assureur*** se réserve expressément le droit d'exercer tout recours subrogatoire à l'encontre de ces sociétés ou personnes.

Les mandataires sociaux salariés de l'***assuré*** sont également considérés comme ***préposés***. [non consolidé]

PRESTATAIRE D'EXTERNALISATION

Toute entité extérieure à l'assuré à l'exception du prestataire de service de cloud et qui lui fournit des services déterminés dans la limite des missions qui lui ont été confiées, notamment un service externalisé de gestion de la paie, d'hébergement web, de marketing ou de prospection, qu'elle agisse ou non en vertu d'un engagement contractuel exprès. [non consolidé]

RÉCLAMATION

Toute mise en cause expresse fondée sur une ***faute professionnelle***, réelle ou alléguée, à l'encontre de l'***assuré*** pendant la ***période d'assurance*** prolongée le cas échéant par la période de garantie subséquente.

Est assimilée à une ***réclamation*** toute déclaration faite par l'***assuré*** à l'***assureur*** concernant des dommages ou évènements susceptibles de relever des garanties du présent contrat. [non consolidé]

SANCTION ADMINISTRATIVE

Amendes et pénalités : sanctions d'ordre pécuniaire encourues par l'assuré à la suite d'une méconnaissance de ses obligations légales, réglementaires ou prudentielles, de nature civile, pénale, administrative ou contractuelle.

- Amendes civiles (ou à des dommages et intérêts pour action dilatoire ou abusive (article 32-1 CPC) ou pour appel dilatoire ou abusif (article 559 CPC) : elles ne sont pas assurables. Il s'agit de la condamnation à des dommages intérêts pour procédure abusive (application particulière du droit de la responsabilité civile pour faute). Il s'agit de sanctionner l'abus d'exercice du droit d'ester en justice ou d'interjeter appel.
- Amendes pénales : elles ne sont pas assurables et proviennent d'une condamnation prononcée par une juridiction répressive.
- Amendes administratives : elles ne sont pas assurables. Sanctions pécuniaires prononcées par des autorités administratives indépendantes ayant un pouvoir de sanction et après constatation du non-respect de règles prudentielles, légales ou règlementaires [APSAD].

Toute sanction pécuniaire assurable infligée à l'***assuré*** par un organisme gouvernemental, un organisme officiel, une instance administrative, institué en application des règlementations de protection des ***données*** (notamment la CNIL en France), en conséquence d'une violation de la règlementation sur la protection, conservation, confidentialité des ***données***.

SÉCURITÉ DES SYSTÈMES D'INFORMATION

Ensemble des mesures techniques et non techniques de protection permettant à un système d'information de résister à des événements susceptibles de compromettre **la disponibilité, l'intégrité ou la confidentialité** des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. [ANSSI]

SERVICE DE CLOUD

Tout accès à des infrastructures ou plates-formes informatiques hébergées chez un prestataire informatique avec lequel l'***assuré*** a passé une convention à cet effet. [non consolidé]

SINISTRE

Garantie pertes et frais :

- La connaissance par l'***assuré*** d'une ***atteinte aux données***.

Garantie responsabilité civile :

- Toute ***réclamation*** adressée à l'***assuré*** ou à l'***assureur***.

Constitue un seul et même ***sinistre*** tout dommage ou ensemble de dommages causés à des ***tiers*** engageant la responsabilité de l'***assuré***, résultant d'un ***fait dommageable*** et ayant donné lieu à une ou plusieurs ***réclamations***. [non consolidé]

SYSTÈME D'INFORMATION

Ensemble organisé de ressources (**matériels, logiciels, personnel, données et procédures**) permettant de traiter et de diffuser de l'information. [ANSSI]

Matériel, équipement informatique, logiciels (et leurs composants) qui font partie intégrante d'un système ou d'un réseau accessible par internet ou réseau intranet ou connecté à une plateforme de stockage ou tout appareil périphérique exploité par l'***assuré*** ;

Tout ordinateur ou système électronique d'un ***tiers*** utilisé pour accéder au ***système d'information*** ou aux données stockées dans le ***système d'information.***

Toute plate-forme de stockage ou de traitement et tout autre appareil périphérique ou ***système d'information*** appartenant à, contrôlé, exploité ou loué par un ***prestataire d'externalisation***.

Les ***services de cloud*** utilisés par l'***assuré***. [non consolidé]

TIERS

Toute personne autre que le ***souscripteur*** et, dans l'exercice de leurs fonctions, ses représentants légaux et ses ***préposés***. [non consolidé]