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

RÉSULTATS de la RECHERCHE

Année 2
Séminaire février 2017 - octobre 2017

RAPPORT

ÉTABLI PAR

PHILIPPE COTELLE RISK MANAGMENT INSURANCE AIRBUS DEFENCE AND SPACE in charge of Cyber Risk for AIRBUS	PHILIPPE WOLF PROJECT MANAGER IRT-SYSTEMX	BENEDICTE SUZAN Rédacteur principal R&T & INNOVATION Cooperation AIRBUS DEFENCE AND SPACE

EN PARTENARIAT AVEC

POUR TOUT RENSEIGNEMENT CONCERNANT CE RAPPORT, VOUS POUVEZ CONTACTER L'IRT SYSTEMX AUX COORDONNÉES SUIVANTES : IRT SystemX 8, avenue de la Vauve CS 90070 – 91127 Palaiseau Cedex
Site internet : www.irt-systemx.fr Courriel : philippe.wolf[at]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[at]irt-systemx.fr

Table des matières

I. Présentation des travaux 5
II. Résumé de la démarche 11
III. Recommandations consolidées 13
Recommandation 1 13
Recommandation 2 13
Recommandation 3 13
Recommandation 4 13
Recommandation 5 13
Recommandation 6 13
Recommandation 7 13
IV. Résumé des résultats de la recherche 14
V. Méthode suivie pour la recherche 18
VI. INTRODUCTION 21
VI.1. Constat 21
VI.2. Objectifs de la recherche 22
VII. La Prise en compte du risque cyber par les agences de notation financière 25
VII.1. *Considerations on Cyber Risk* : perception et prise en compte du risque cyber 25
VII.1.a. Le risque cyber se situe désormais en haut des agendas des compagnies d'assurance et de réassurance 25
VII.1.b. Intégration du risque cyber dans la notation 26
VII.1.c. L'approche d'A.M. Best dans sa prise en compte du risque cyber pour l'exercice de notation 27
VII.1.d. Le risque cyber et la notation des entreprises d'assurance : les prochaines étapes 29
VII.2. Comment les risques cyber sont-ils pris en compte et peuvent influencer la notation d'une organisation ? .. 30
VII.2.a. Présentation de l'organisation 30
VII.2.b. Présentation générale des méthodes de notation 30
VII.2.c. Les éléments intangibles pris en compte à ce jour par Moody's 31
VII.2.d. Focus sur le risque cyber 31
VII.2.e. Les principaux cas d'attaque cyber qui ont fait l'objet d'un commentaire 33
VII.2.f. La prise en compte par Moody's du risque d'accumulation 34
VII.2.g. Appréciation du rôle des États face au risque cyber 34
VII.2.h. La tendance de la prise en compte du risque cyber 35
VIII. La responsabilité des dirigeants face au risque cyber 36
VIII.1. La responsabilité des dirigeants face au risque cyber, le cadre légal et réglementaire 36
VIII.1.a. Focus sur le cadre légal en matière de protection des données à caractère personnel (LI&L) 36
VIII.1.b. Quelle responsabilité pour les dirigeants d'entreprise 39
VIII.1.c. Comment limiter la responsabilité des dirigeants face aux dispositions du RGPD ? 40

VIII.2. La responsabilité des dirigeants face au risque cyber, le transfert vers l'assurance, *AIG* 42
VIII.2.a. Les points essentiels de la couverture 42
VIII.2.b. Les acteurs de la mise en cause des dirigeants 43
VIII.2.c. Les acteurs de la mise en cause des dirigeants lors d'un incident cyber 44
VIII.2.d. Responsabilité des dirigeants dans les grandes entreprises : la communication financière 46
VIII.2.e. Les challenges pour l'industrie de l'assurance 47
VIII.2.f. Retour d'expérience sinistre Cyber : la gouvernance, un élément clé 48
IX. La valorisation des biens intangibles et leur gestion d'un point de vue assurantiel 50
IX.1. Les fondamentaux de la valorisation comptable des données intangibles 50
IX.1.a. La part de la valeur des biens intangibles dans les entreprises ne cesse de croître 50
IX.1.b. Comptabilisation des coûts de développement en interne entreprise 52
IX.1.c. La valorisation des biens intangibles, une approche par les revenus pour les marques et les brevets. . 54
IX.1.d. L'assurance peut-elle assurer la confiance ? 56
IX.2. Risque, audit et contrôle interne, l'organisation du management des risques dans la gestion d'entreprise et les documents obligatoires 56
IX.2.a. Le management des risques, l'audit et le contrôle des risques dans les grandes entreprises – rôles et responsabilités 56
IX.2.b. Les critères de comptabilisation d'un risque au bilan sont restreints 58
IX.2.c. Comment amener les entreprises à structurer leur démarche ? 58
IX.3. Le traitement par le juge judiciaire de l'indemnisation des préjudices immatériels 63
IX.3.a. Le préjudice immatériel et l'indemnisation. Principes 63
IX.3.b. Le chiffrage du préjudice par le juge 63
IX.3.c. L'évolution législative, vers l'élargissement de l'indemnisation des préjudices, l'exemple de l'atteinte au droit de la propriété intellectuelle. Principes. 64
IX.3.d. L'évolution jurisprudentielle vers la réduction de l'indemnisation des préjudices : le fait fautif des « victimes informatiques » 67
IX.3.e. La préparation du traitement judiciaire commence avant la crise 68
X. La réponse de l'assurance (et de la réassurance) pour couvrir les biens tangibles et intangibles 70
X.1. Première étape : sécuriser les nouveaux produits d'assurance cyber 70
X.1.a. Retour d'expérience sur la mise en place de programmes d'assurance cyber à vocation de masse 70
X.1.b. La stratégie du Lloyds de Londres pour l'assurance du risque cyber 75
X.2. La réponse des Assurances et de la Réassurance sur l'assurabilité des intangibles 78
X.2.a. La position de la FFA 78
X.2.b. L'intangible entre une approche traditionnelle et progressiste 80
XI. Comment est-ce que la réassurance peut avancer sur l'assurance des biens intangibles 82
XI.1. Les réflexions pour la réassurance 82
XI.1.a. Les chiffres du marché 82
XI.1.b. Les couvertures du cyber risque 82

XI.1.c. Un paysage assurantiel changeant et diversifié 83
XI.1.d. Les limites de l'assurabilité 83
XI.2. Position de l'APREF – comité système d'information : les potentielles difficultés au développement du marché de la cyber assurance 85
XI.2.a. Où se situent les spécificités de l'assurance cyber ? 85
XI.2.b. Le cumul du risque n'est pas maîtrisé 86
XI.2.c. Fluidifier pour améliorer le marché 88
XI.2.d. Les pistes, les travaux des réassureurs 89
Annexe 1 – La notion d'incident de sécurité à travers les normes et les textes réglementaires 91
Annexe 2 – Le résumé du cadre réglementaire sur la Sécurité des Systèmes d'information 94
Annexe 3 – Assurance d'une infraction ou d'une sanction : la réponse en droit français 96
Annexe 4 – Note sur l'assurabilité des amendes administratives 98
Annexe 5 – Avant-projet de réforme du droit des obligations (septembre 2005) 99
Annexe 6 - Bibliographie 100
Annexe 7 – La réponse des assureurs et des réassureurs à WannaCry 103
Le principe indemnitaire traditionnel et le cyber 103
La gestion de la crise WannaCry par les assureurs 103
Annexe 8 - Présentation succincte des résultats année 1 104
Annexe 9 – Les recommandations issues du premier rapport 106
Annexe 10 – Tableau de suivi des recommandations (année 1) soit reprises dans d'autres documents soit qui ont fait l'objet d'actions 109
Annexe 11 – Travaux ultérieurs (année 3) 111
Annexe 12 – La lettre d'invitation 112
Annexe 13 – L'IRT-SystemX 113
Annexe 14 – Le projet EIC 114
Annexe 15 – Les participants 116
Annexe 16 – Groupe de travail 117

I. Présentation des travaux

Dans le cadre de son projet EIC[1] (Environnement pour l'Interopérabilité et l'Intégration en Cybersécurité), l'IRT-SystemX mène des travaux sur **la maîtrise du risque cyber** dans une approche pluridisciplinaire croisant sciences mathématiques et informatiques avec sciences économiques, sociales et du comportement.

Sous l'impulsion du *Security Officer* d'**AIRBUS** et du Directeur général de l'**ANSSI** (Agence nationale de la sécurité des systèmes d'information), l'IRT-SystemX anime depuis novembre 2015 un groupe de travail sur « La maîtrise du risque cyber sur l'ensemble de la chaîne de sa valeur et son transfert vers l'assurance ». Il réunit des spécialistes de l'assurance et de la réassurance, des courtiers, des juristes, des actuaires, des industriels (*risk managers*), des experts de l'OCDE, sous l'égide de la Fédération Française de l'Assurance (FFA), de l'association française des professionnels de la réassurance en France (APREF), de *The Federation of European Risk Management Associations* (FERMA) et de l'association française des professionnels de la gestion des risques et des assurances (AMRAE).

Un **premier rapport de recherches**[2] a été rédigé et publié fin juillet 2016 (en français et en anglais).

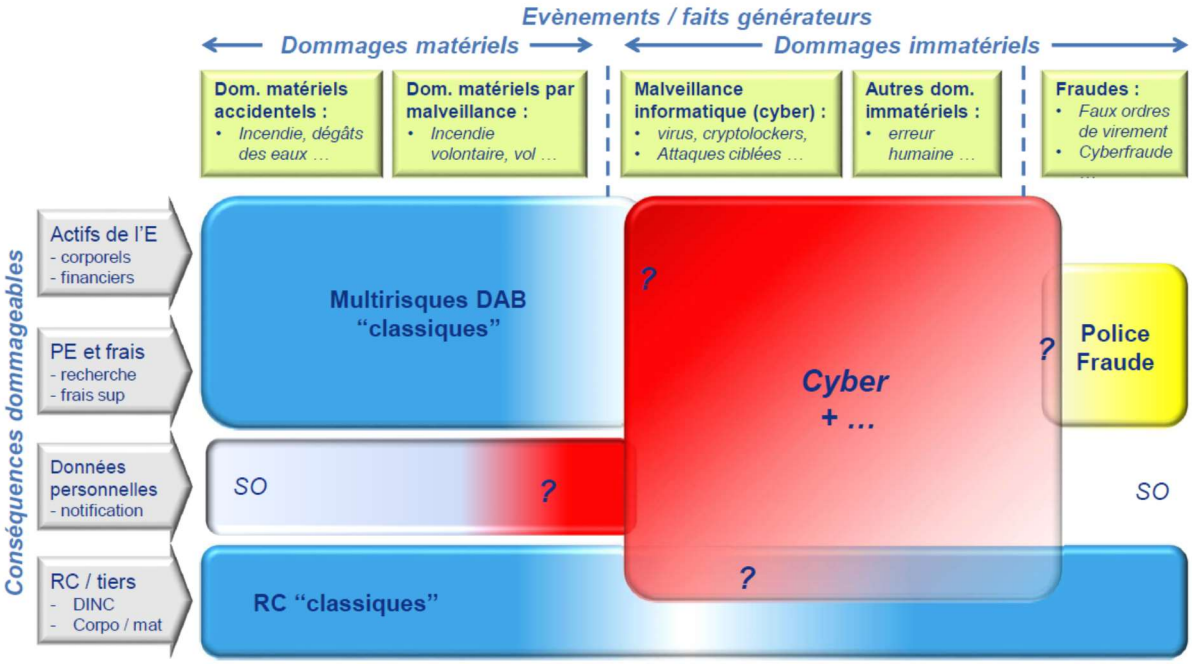


Figure 1 - Matrice synthétique Faits générateurs dommageables / Garanties

Le **deuxième cycle de séminaires** en 2017 traite principalement de **la valorisation des données intangibles conditions nécessaires pour connaître, gérer et maitriser le risque cyber pour ensuite le transférer éventuellement vers l'assurance**. Le chapitre II résume **les résultats obtenus**. Le chapitre III liste **des recommandations**. Les chapitres ultérieurs détaillent l'ensemble des réflexions menées. Nous privilégions dans ces chapitres un exposé de l'exhaustivité des débats, comme matière première et parfois brute pour des travaux ultérieurs ou connexes. Nous posons des questions dont beaucoup n'ont pas de réponse aujourd'hui. Les annexes décrivent le contexte de ces travaux, les matériaux utilisés et quelques retombées concrètes. Les

[1] Voir http://www.irt-systemx.fr/project/eic/

[2] Voir http://www.irt-systemx.fr/publications/english-la-maitrise-du-risque-cyber-sur-lensemble-de-la-chaine-de-sa-valeur-et-son-transfert-vers-lassurance/

réflexions ont principalement porté sur les grandes entreprises mais doivent être étendues aux ETI et aux TPE/PME.

La grille de travail initiale pour l'année 2, ci-après, 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
Seconde Année de la recherche (3 ans envisagés)	La seconde année est consacrée à la gouvernance du risque cyber et son transfert vers l'assurance avec un focus particulier sur question de la valorisation des données intangibles par les acteurs qui valorisent l'entreprise.				Le secrétariat des séances et la production écrite est assurée par EIC.
1er réunion 2h30 Février	Présentation rapide des résultats de la recherche année 1 et présentation de la proposition de recherche pour la seconde année. Présentation du point de vue du Risque Manager et du marché de l'assurance : nécessité d'avancer sur la gouvernance du risque et la culture du risque : comprendre la valorisation des données intangibles.	Présentation du calendrier, des réunions et des thèmes de l'année. Début des travaux. Comment les auditeurs, les agences de notation, la Finance et le contrôle de gestion, les Commissaires aux comptes et l'ACPR valorisent les données intangibles et le risque cyber dans un objectif de gestion et de transfert du risque vers l'assurance.	Recueil d'information : ce dont ont besoin les parties prenantes invitées pour valoriser les biens intangibles afin de gérer le risque cyber. Démontrer l'utilité d'un dialogue entre les acteurs de la valorisation de l'entreprise, le risk manager et le marché de l'assurance. Quels sont les points de blocages ? Comment avancer ? Accord sur la finalité de la recherche	Compte rendu de séance. Road map, calendrier des activités et des apports des parties prenantes.	Appel à contribution auprès des partenaires.
2e réunion 2h30	Quels sont les risques cyber pour les membres des conseils d'administration ? Comment est-ce que l'on définit la	Que dit le régulateur ? Que dit la conformité ? Quelles sont les attentes des actionnaires ?	Mapping des compétences en interne organisation pour répondre aux enjeux de la gouvernance du risque digital. Mapping des compétences en externe.	Compte rendu de séance. Rapport de de synthèse illustrant les problématiques et le consensus obtenu exposant les avancées de la réflexion.	

	gouvernance digitale pour une organisation pour savoir quels vont être les risques cyber qui vont être acceptés ou retenus ?	Quels risques juridiques de tiers ? Comment avancer ? Quels sont les points de blocages ?	Est-ce que le Digital Officer répond aux enjeux ? Faut-il créer des Digital Advisory Board		
3e réunion 2h30	L'analyse du risque cyber pour le conseil d'administration ? Quels éléments financiers présenter ? Sous quelle forme, issue de quelle démarche ? Comment est-ce que l'on cadre la démarche SPICE pour qu'elle réponde aux besoins des acteurs de la valorisation de l'entreprise ?	Rependre le tableau « matrice des couvertures d'assurance du marché » et sur la démarche SPICE qui permet de définir l'exposition financière au risque cyber. L'enjeu d'une méthodologie partagée par les parties prenantes pour développer la gouvernance et le transfert du risque. Quelle quantification pour les risques élémentaires identifiés dans la matrice ? Quelle formule de calcul pour chaque cellule de risque élémentaire ?	Produire les premiers éléments d'une méthode, d'un mode de calcul et des règles qui puissent être agréés par les parties prenantes. Qu'est-ce que l'entreprise est-elle capable de fournir afin de valoriser les biens intangibles ?	Compte rendu de séance. Document synthétique illustrant les problématiques et le consensus obtenu exposant les avancées de la réflexion.	
4e réunion 2h30	Comment est-ce que l'assurance peut répondre aux risques intangibles ?	Est-ce que les assureurs sont prêts à réfléchir autrement concernant le risque cyber ? Quelle réponse peuvent-ils apporter sur base de la valorisation des données intangibles ?	Définir les conditions de la valorisation des biens intangibles par le marché de l'assurance.	Compte rendu de séance.	

	Quelle est l'exposition des besoins des assureurs face aux réponses des acteurs de la valorisation des biens immatériels ?	Avec les éléments réunis lors des réunions 1, 2 et 3, est-ce que les assureurs sont en mesure de mieux définir leur évaluation de l'exposition au risque digital et cyber ?	Définir les éléments d'une modélisation pour indemniser l'assuré pour ce genre de sinistre.	Document synthétique illustrant les problématiques et le consensus obtenu exposant les avancées de la réflexion.	
5e réunion	Assurance et Re assurance : Comment est-ce que les résultats des réunions 1, 2, 3 et 4 se mettent en place ? Les résultats obtenus peuvent-ils conduire à la définition d'une nouvelle offre ? Vers une nouvelle matrice de la couverture du risque cyber ? L'enjeu de la capacité.	Quelles sont les informations nécessaires ? Comment gère-t-on la souscription ? Comment se gèrent les sinistres ? Comment est-ce qu'on met en place des capacités financières à la hauteur des enjeux financiers du risque digital cyber pour l'assurance et la re assurance ? Comment faire pour que ce risque soit porté de manière crédible ? Comment est-ce que l'on fait pour rassembler des capacités pour que l'assurance ait du sens ?	Liste de pistes d'évolutions envisageables, trends probables, résultats prospectifs réalistes pragmatiques.	Compte rendu de séance. Document synthétique illustrant les problématiques et le consensus obtenu exposant les avancées de la réflexion.	
6e réunion	Risque d' accumulation Risque systémique	Identifier les risques cumulés. Décomposer les risques	Définir le périmètre des couvertures d'assurance cyber.	Compte rendu de séance. Document synthétique	

		élémentaires des scénarios de risque dans la matrice. Comment exploiter ces résultats d'un point de vue statistique ?		illustrant les problématiques et le consensus obtenu exposant les avancées de la réflexion.	
7e 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 pour validation par les parties prenantes. Présentation du plan d'action pour diffuser les résultats de la recherche et communiquer. Présentation des moyens nécessaires pour ce faire.	

Figure 2 – Plan de travail

II. Résumé de la démarche

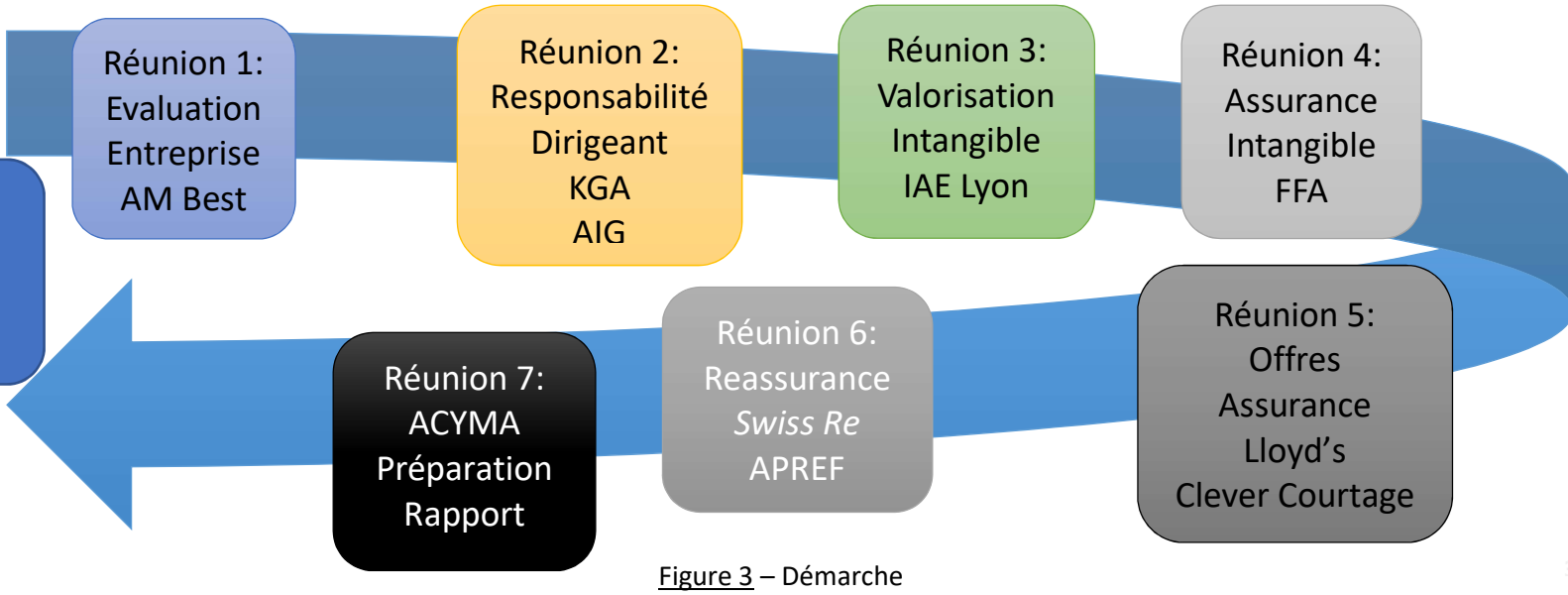


Figure 3 – Démarche

La digitalisation est le moteur de la croissance économique des entreprises. Elle a pour conséquence une augmentation de la part des biens intangibles dans la valorisation financière des entreprises. Ces biens intangibles sont, par essence, plus sensibles et plus exposés au risque cyber. A ce jour, il n'y a pas de solution de transfert et de financement du risque par des solutions d'assurance.

La démarche de cette année de recherche a consisté à réfléchir ensemble avec les acteurs de marché sur cette situation et d'évaluer les étapes qui permettraient à l'avenir d'explorer de nouvelles solutions d'assurance.

Il s'agissait donc en premier lieu de rechercher à objectiver, caractériser et valoriser ces biens intangibles en fonction des attentes des professionnels consultés comme les agences de notation, les auditeurs, comptables, experts comptables, avocats, professeurs d'université. Cette étape nous a permis de mettre en lumière la part prépondérante des biens intangibles dans la valeur financière des entreprises tout en montrant que celle-ci ne figure pas, pour la plus grande part, au bilan des sociétés.

On a néanmoins pu mettre en valeur d'autres méthodes objectives de valorisation des biens intangibles que ce soit dans le cadre d'opérations d'acquisition ou de décisions de justice.

Assureurs et réassureurs ont pu s'exprimer sur leur position face à ce problème. Ils ont montré leurs difficultés à étendre de manière généralisée les couvertures cyber actuelles aux biens intangibles. Le lien objectif entre l'évènement cyber et une dégradation permanente de la valeur financière de ces biens intangibles en est un des principaux challenges.

Cependant, les recherches dans ce domaine continuent. Assureurs et réassureurs ont montré que des voies nouvelles comme l'assurance paramétrique ou indicielle pouvaient être explorées sous réserve d'un travail conjoint avec les entreprises pour associer de manière objective une valeur financière aux différents biens intangibles.

Le marché de l'assurance cyber aujourd'hui fait face à d'autres challenges comme la modélisation du risque et l'accumulation qui réduisent leur disposition à explorer ces nouvelles voies alors que ces fondamentaux ne sont pas raffermis – donner un prix au risque et gérer son exposition.

Les entreprises elles-mêmes sont pour beaucoup réticentes à valoriser financièrement leurs biens intangibles. Il semble néanmoins probable que sous la pression des investisseurs, des agences de notation et du régulateur, les entreprises doivent donner plus de visibilité sur ces aspects, de même sur leur capacité à protéger ces valeurs et à être résiliente en cas d'attaques.

La gestion du risque cyber va avoir un impact de plus en plus important sur la valorisation financière des entreprises. Cette gestion inclut une identification et une quantification financière du risque, impose une gouvernance, ainsi que des mesures de protection, de défense et de résilience dans le cadre d'un standard international pour lequel Airbus, l'ANSSI, FERMA et l'AMRAE sont proactifs sur la scène internationale.

Les recommandations ci-dessous, sont le résultat des discussions.

III. Recommandations consolidées

Recommandation 1

Sensibiliser les organisations pour augmenter la maturité de l'entreprise à la gouvernance du risque cyber ainsi qu'à son exposition à ces risques, mettre en place les investissements pour prévenir, protéger et remédier à la survenance d'un acte de cyber malveillance ainsi que de financer le risque, notamment par le recours aux solutions d'assurance.

Le chapitre VII développe cette recommandation.

Recommandation 2

Proposer un cadre sur la communication externe des entreprises sur le risque cyber et leur exposition.

Le chapitre VIII développe cette recommandation.

Recommandation 3

Clarifier les obligations et les responsabilités des dirigeants et leur protection dans le cadre des polices D&O (*Directors and Officers Liability Insurance*) sur le risque cyber.

Le chapitre VIII développe cette recommandation.

Recommandation 4

Proposer des normes internationales sur l'évaluation financière d'un impact sur les biens intangibles de l'entreprise.

Le chapitre IX développe cette recommandation.

Recommandation 5

Comment travailler avec les assureurs sur le développement de solutions assurantielles pour les biens intangibles ?

Le chapitre IX développe cette recommandation.

Recommandation 6

L'offre d'assurance cyber des bien tangibles se structure pour mieux répondre aux besoins de l'entreprise, comment le communiquer, comment comparer ?

Le chapitre X développe cette recommandation.

Recommandation 7

Développer l'accès aux données pour la modélisation du risque cyber et clarifier le risque d'accumulation pour permettre à la réassurance d'être un moteur d'expansion de ce marché.

Les chapitres X et XI développent cette recommandation.

IV. Résumé des résultats de la recherche

Les travaux ont porté sur des sujets innovants et complexes comme les biens intangibles abordés du point de vue des porteurs du risque. Quelle est aujourd'hui leur préoccupation et comment le risque cyber fait partie de la sensibilité financière des entreprises et de leurs dirigeants.

Thèmes traités lors de la première séance

Les agences de notation ont fait part de leur volonté de prendre ce risque en compte et leurs difficultés actuelles à le modéliser.

La première séance montrait la façon dont le risque cyber était appréhendé par les agences de notation. Aujourd'hui, l'état de l'art montre que le risque cyber est difficile à prendre en compte par les agences de notation. Il présente un risque de cumul certain qui est difficile à appréhender.

Dès 2016, *Moody's* indique qu'elle évaluera dans quelle mesure les entreprises continuent de développer une « culture de défense » face au risque cyber. L'agence s'attend à ce que les sociétés ne fassent pas seulement ce qui est attendu d'elles au regard des dispositions réglementaires, légales et de conformité compte tenu de la nature évolutive de la menace cyber. **Le règlement, la disposition légale deviennent ainsi un risque si les sociétés ne font qu'adhérer à une culture de conformité.**

La capacité du secteur des assurances à mitiger le risque est en développement. *A.M. Best* continue à développer sa compréhension de la manière dont les compagnies prennent en compte le risque cyber à la fois en interne (le point de vue de l'utilisateur) et en externe (le point de vue du vendeur).

Une pression existe sur les agences de notation pour **prendre en compte le cyber risque dans leur notation** sur la stratégie et **la réputation de l'entreprise**. Certes d'autres éléments rentraient en cause, **mais le lien entre attaque cyber et perte d'opportunité (actif intangible) sur des éléments attendus a été fait**.

Pour le moment, le risque cyber est essentiellement analysé en tant qu'*event risk* par les agences de notation – un évènement difficile à chiffrer a priori – mais sur lequel une analyse des conséquences a posteriori peut être menée.

Cela présente un certain nombre de défis qui pourraient conduire à une approche potentiellement plus large de la notation de sorte à pouvoir intégrer des risques de cumul nouveau émergents tels que ceux présentés par l'exposition au risque cyber. L'approche par **sinistre maximum possible** (SMP) et donc par engagement cumulé total pour un seul évènement pourrait être utilisée pour stresser les bilans des assureurs comme cela est fait actuellement sur les évènements catastrophiques plus traditionnels tels que catastrophe naturelle (CATNAT) et terrorisme.

Le risque cyber est désormais incontournable ; **les méthodologies** pour sa prise en compte **vont encore évoluer**, **le benchmark des sociétés va se développer**.

Les entreprises seront de plus en plus challengées sur les impacts des risques sur leur situation financière et leur capacité de crédit. L'analyse pourrait de plus en plus prendre en compte des évènements prospectifs.

Le ***risk management* pourra être apprécié de façon qualitative par des éléments culturels**, un *trade record*. **Les éléments quantitatifs pourront être amenés par la quantification des scénarios catastrophe développés en interne par l'organisation et par le montant des sanctions prévues en cas de non-respect**. Enfin, la preuve

de la conformité aux règlementations et normes est nécessaire mais pas suffisante. La normalisation et la compliance deviennent un risque pour la réponse à apporter à la gestion du risque cyber.

Thèmes traités lors de la seconde séance

La seconde réunion avait pour objectif de mettre en lumière l'exposition des dirigeants face au risque cyber. Comment les dirigeants pouvaient percevoir ce risque par rapport à leur propre responsabilité. D'où la présentation du cadre réglementaire qui incite et invite à une gouvernance du risque cyber comme un élément important des entreprises. Ce cadre réglementaire accentue l'exposition des dirigeants face au risque cyber.

Les signaux actuels montrent que le cyber restera couvert par la police D&O (Assurance Responsabilité Civile des Dirigeants et des Administrateurs). La nature des terrains de la mise en cause concerne : le social, le fiscal, le réglementaire, le boursier, le cyber, l'environnement…

Un point d'attention demeure si les recours contre les dirigeants se multiplient et si les contrats D&O sont de plus en plus activés, le domaine cyber restera-t-il couvert ?

Questions

En supposant que le risque cyber continue d'être couvert dans les polices D&O, **est ce que la gouvernance du risque cyber peut être un critère de souscription** ? Peut-on éventuellement pousser les entreprises et les dirigeants à démontrer qu'une gouvernance a été mise en place de façon à pouvoir bénéficier de cette couverture D&O. Une réponse possible apportée par *AIG* – les souscripteurs cyber ne sont pas les mêmes que les souscripteurs D&O lesquels aujourd'hui n'insèrent pas encore de critères ni de questions sur le niveau de connaissance des dirigeants et s'ils ont mis en place des bonnes pratiques.

Quelques critères pourraient être rajoutés ? Comme pour le blanchiment, les contre parties financières, le risque crédit, le risque politique, la diversité sociale.

D&O et assurabilité des peines civiles et administratives ? (voir de plus les chapitres détaillés).

Un point inquiétant existe sur les responsabilités qui pèsent sur les dirigeants (RGPD – Règlement Général de Protection des Données, Loi Sapin…). **Le projet de réforme du code de la responsabilité civile pourrait clarifier ce qui pourrait être assurable ou pas**. Le législateur doit également s'exprimer sur l'intérêt d'une clarification – entre les deux notions de contradiction à l'ordre public et moralité de la chose.

Le critère reste celui de la moralité. Si la condamnation d'une administration n'est pas associée à une autre condamnation, pouvons-nous considérer que la pénalité administrative n'est pas la contrepartie d'une peine et qu'à ce titre-là elle puisse être indemnisée. Le débat est posé.

Au vu de l'évolution du cadre juridique et réglementaire, le risque cyber doit être au cœur des préoccupations des dirigeants cyber (en interne) mais également dans **les risques accrus de mise en cause de la responsabilité des dirigeants d'entreprise du fait de ces nouvelles obligations** ainsi que présenté par *KGA, Avocats*.

La responsabilité des membres du conseil d'administration pourrait être engagée sur le terrain de la faute de gestion, la faute la plus communément reprochée aux administrateurs étant le défaut de surveillance de la direction (faute de négligence). **D'où l'importance pour les conseils d'administration d'inscrire ce risque.**

Les obligations issues du RGPD – Règlement Général de Protection des Données : un nouveau paradigme de responsabilité.

Le **RGPD introduit en droit français les concepts d' « *accountability* » et de *« privacy by design »*.** La notion d'« ***accountability*** » **désigne l'obligation pour les entreprises de mettre en œuvre des mécanismes et des**

procédures internes permettant de démontrer le respect des règles relatives à la protection des données. La notion de « ***privacy by design*** » **implique que les enjeux liés à la protection des données soient envisagés dès l'origine de tout projet comprenant un traitement de données à caractère personnel** puis, ensuite, **tout au long des différentes étapes de conduite de ce projet**.

Thèmes traités lors de la troisième séance

La réunion souhaite apporter un nouvel éclairage sur la valorisation des biens intangibles et leur gestion d'un point de vue assurantiel même si ils ne sont pas formellement présents au bilan des sociétés. Néanmoins, ils sont valorisables et peuvent être reconnus en cas de perte. Trois interventions ont abordé ce sujet.

La première présentation par le Professeur Edouard Chastenet traite de la façon dont les biens intangibles sont comptabilisables et comment leur apporter une valeur financière objective, un élément important pour l'appréciation, par l'assurance, des biens intangibles.

Le cabinet *EY* montre comment les risques sont reconnus dans les bilans des organisations et notamment les risques cyber.

Enfin, les cabinets *CleverCourtage et LCA – ICSI* exposent comment sont actuellement indemnisés les risques intangibles devant les tribunaux. La façon dont les juges judiciaires appréhendent la réparation des préjudices immatériels liés à l'économie numérique traduit une évolution similaire à celle qui a conduit la jurisprudence à admettre l'existence, à côté d'un principe de responsabilité pour faute, d'une responsabilité sans faute. La question qui leur est posée est de savoir s'ils ont bien pris la mesure des enjeux posés par les nouvelles technologies. On pourrait penser le contraire à la lecture de certains auteurs qui déplorent la faiblesse des dommages-intérêts accordés par exemple en matière de contrefaçon par les magistrats qui raisonneraient trop selon des schémas classiques. En réalité, si le principe de la réparation du préjudice immatériel ne pose pas de difficulté, c'est en revanche le contenu de celui-ci qui fait débats. C'est donc davantage la question de la preuve de ce préjudice qui se pose, ce qui rejoint ici aussi en matière judiciaire notre débat sur la qualification et la quantification de l'immatériel.

Questions

La logique de ces trois interventions est d'essayer d'abord de mieux reconnaitre la valeur des biens intangibles afin que ces éléments puissent devenir un élément de calcul de la prime (l'assiette de la prime) par le marché de l'assurance. Ensuite, la question posée fut de savoir si et comment les solutions d'assurance qui existent actuellement pourraient être utilisées par les sociétés dans le cadre de leur communication financière et ce, à leur avantage. **Est-ce que l'assurance pourrait être perçue comme une création de valeur pour les sociétés ?** Enfin, eu égard aux sinistres, comment peut-on établir un lien de cause à effet entre une occurrence et un sinistre et, comment le sinistre peut être valorisé. Ce lien entre fait générateur et conséquence dommageable est un des éléments clefs à résoudre pour les assureurs.

Il était attendu des trois interventions qu'elles apportent des éléments de réflexion pour envisager quelles sont les pistes qui s'offrent pour développer de nouvelles solutions assurantielles pour les biens intangibles lesquels constituent, dans le cadre d'une économie digitalisée, une part très importante, voire la plus importante de la valeur d'une entreprise. **Comment traduire tous ces éléments en couverture d'assurance ?**

Thèmes traités lors de la quatrième, cinquième et sixième séance

Une première réponse du marché de l'assurance a exprimé son intérêt pour se pencher sur ces questions et en même temps, la difficulté d'y apporter une réponse à court terme. Les entreprises ne semblent pas être prêtes à payer ou très peu pour les conséquences d'évènements cyber qui se traduisent par la dépréciation de biens intangibles. L'assurabilité des biens tangibles à la suite d'actes de cyber malveillance est assurable. Il est beaucoup plus difficile d'appréhender l'assurabilité des biens intangibles et cela d'une manière générale quel que soit le fait générateur et pas uniquement en cas de fait générateur cyber. Tant qu'il n'y aura pas de prise de conscience de certains évènements très importants qui pourront être indemnisés par la couverture d'assurance, cela va être compliqué.

Les débats n'ont pas permis d'avancer cette année sur les verrous suivants :

Les verrous : le lien de causalité entre le fait générateur et les conséquences dommageables ; le fait dommageable cyber n'est généralement pas le seul évènement qui concoure à la dépréciation du bien intangible. D'autres facteurs entrent en ligne de compte ; quel critère pour quantifier le bien intangible ?

Pouvons-nous dès à présent associer à chaque cellule une norme et une formule pour développer la quantification ? Peut-on tester la matrice avec un auditeur ?

On ne couvre pas le risque cyber en lui-même mais on parle de l'indemnisation du risque juridique, administratif de la notification consécutive à une fuite de données massive (*data breach*). C'est parce qu'il y a les études du *Ponemon Institute*[3], une valorisation des impacts de la législation et que le coût de la notification est connu que l'on a réussi à quantifier la conséquence. On ne couvre pas le fait générateur mais une des conséquences.

Le débat central est **quelle est la valeur de l'information ?**

Un sondage de l'association britannique des *risk managers* paru en juin 2017, positionne le risque cyber sur les biens intangible (réputation) en première position. Comment le marché de l'assurance et les services des *risk managers* peuvent-ils innover pour répondre à cette exposition.

Model asset free = la richesse de l'entreprise réside dans le savoir et la propriété intellectuelle.

Le marché de l'assurance a toujours eu comme objectif de protéger la valeur des assurés. Elle était tangible jusqu'à peu. L'évolution se fait désormais vers la valorisation de la donnée. Les efforts vers la recherche de solutions sont un élément important de préoccupation pour l'ensemble des porteurs de risque et des *risk managers* des grandes sociétés.

Le marché réfléchit aujourd'hui à comment répondre aux attentes des assurés autour de la question faut-il des polices dédiées ou incluses dans les polices traditionnelles (JLS). La vision du marché des Lloyds apporte un éclairage intéressant sur les réponses nouvelles.

[3] Il convient néanmoins de s'interroger sur l'application de la méthode utilisée (*activity-based costing*) aux entreprises françaises, voir http://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2017_Global_CODB_Report_Final.pdf?t=1510933508399

V. Méthode suivie pour la recherche

Ce travail de recherche a été mené par une équipe pluridisciplinaire regroupant assureurs, réassureurs, courtiers, associations professionnelles, juristes, des *risk managers*, des industriels, des organisations internationales, des organismes publics et des chercheurs. Les annexes 13 et 14 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 2. Le plan de travail annuel et les réunions thématiques étaient connus de tous. Envoyé avant chaque réunion, un document préparatoire annonçait les thématiques abordées et les attendus illustrés en séance par les présentations d'experts. Des réunions spécifiques pour approfondir un point posé en séance de travail ont été organisées. Les résultats de la recherche sont le fruit d'un travail collectif réunissant tous les participations du séminaire. Les conclusions et recommandations du rapport de recherche ont ensuite été validées lors de la séance conclusive.

Un consensus a été obtenu autour des **sept recommandations consolidées** du chapitre III. Les chapitres IV à X détaillent la variété des approches et des pistes explorées qui doivent être approfondies dans des travaux ultérieurs décrits à l'annexe 9.

Le séminaire année 2 s'inscrit dans la suite logique des travaux engagés en 2016 et prend appui sur deux de ses recommandations. La première – la nécessité de conduire une analyse de risque interne à l'organisation pour quantifier le risque cyber et sur la troisième – clarifier l'offre aujourd'hui hétérogène entre couvertures classiques et couvertures cyber dédiées.

En effet, maîtriser le risque cyber en interne entreprise et sa quantification financière **nécessite de travailler sur des standards de quantification des risques qui permettront de valoriser l'exposition**. Cette approche permet, dès lors, de justifier les investissements les plus efficaces en cybersécurité pour réduire cette exposition afin que l'organisation puisse être résiliente. **La qualité du *risk management* devenant ainsi un atout de valorisation financière des sociétés, une solution de transfert d'assurance pertinente pourra prendre toute sa valeur**.

Cette perspective permet de travailler avec les assurances de façon à voir comment le marché de l'assurance couvre un besoin dès lors qu'il est mieux défini et quantifié. Le **problème d'accumulation** doit être étudié pour lever les freins des réassureurs à une offre plus ambitieuse.

Trois réunions ont été organisées pour comprendre comment les acteurs de la valorisation de l'entreprise en interne et en externe calculent la valeur qui permet la quantification. Quels sont les facteurs qui sont actuellement pris en compte ou quels seraient ceux qui devraient l'être dans un avenir proche. Une meilleure compréhension de la valorisation des biens intangibles, dont l'importance croît dans une société de plus en plus digitalisée, permettra ainsi de mieux appréhender ce défi de la quantification du risque cyber en vue de son transfert vers l'assurance.

La logique proposée étant la suivante : le risque cyber est le versant négatif des opportunités de croissance que représente la transformation digitale des organisations. Comment intéresser et valoriser la démarche de *risk management* dans les entreprises ? Comment le *risk manager*, dont la fonction est de valoriser le risque, peut-il le faire sur son risque cyber portant sur les données immatérielles de son organisation ? Comment les sociétés vont-elles pouvoir mettre en exergue leur exposition au risque cyber dans la gestion de leurs investissements, la relation avec leur écosystème, leurs clients, les partenaires financiers, les régulateurs … ? Comment vont-elles le prendre en compte après l'avoir identifié, quantifié et valorisé dans leurs bilans ?

La quantification du risque cyber sur l'immatériel suppose qu'un effort de valorisation de l'immatériel ait été conduit en amont comme condition préalable à l'action de valorisation financière que conduit le *risk manager* lorsqu'il quantifie son exposition au risque avant de le transférer à l'assurance.

Inversement, **les acteurs de l'assurance font face aux même défis de la valorisation de l'immatériel lorsqu'ils doivent quantifier leur risque assurable** – les éléments de souscription du contrat d'assurance ; **quantifier l'indemnisation** – l'évaluation de l'indemnité à payer suite au sinistre ; **analyser le caractère systémique du risque** et, inversement, la résilience au risque cyber de l'organisme assuré.

En effet, **il s'agit de comprendre comment les sociétés d'assurance peuvent être à leur tour valorisées** dans leur prise en compte des besoins réels des entreprises et dans leur compréhension du risque. **Quelles sont les informations nécessaires aux assureurs pour déterminer le caractère assurable du risque cyber, le modéliser et déterminer les capacités à mettre en face pour des biens intangibles ? Comment valoriser le sinistre ?** Comment les assureurs et les réassureurs gèrent le cumul ?

Trois réunions ont été conduites pour comprendre comment les acteurs de la valorisation de l'entreprise en interne et en externe calculent la valeur qui permet la quantification des biens intangibles.

Réunion1. Comment les agences de notation prennent en compte le risque cyber dans leur notation ? Quelle est leur perception du risque cyber pour la valorisation des biens intangibles ?

Réunion2. Quels sont les risques auxquels sont exposés les membres des conseils d'administration et les mandataires sociaux de fait ou de droit face au risque cyber. Ces risques sont-ils transférables à l'assurance ? Quelles sont les nouvelles responsabilités imposées par les législations française, européenne ou internationale ? Vers un changement de paradigme ?

Réunion3. Comment se traduit le risque cyber pour le conseil d'administration ? Quelles informations remonter concernant la valorisation des biens intangibles face au risque cyber ? Comment les éléments intangibles et le risque cyber sont-ils pris en compte dans les états comptables et financiers ? Quels éléments financiers présenter ? Sous quelle forme, issue de quelle démarche ?

Trois réunions ont ensuite répondu à la question : comment ces informations permettent au *risk manager* de mieux connaître son risque cyber pour pouvoir mieux le transférer vers l'assurance ? Comment le marché peut-il se saisir de ces informations sur la valorisation des données intangibles ?

Réunion4. Comment est-ce que l'assurance peut répondre au besoin de couverture des risques cyber portant sur les données intangibles ? Quelle est l'exposition des besoins des assureurs face aux réponses des acteurs de la valorisation des biens immatériels ? Il s'agira de poser la limite entre ce qui est transférable et ce qui reste du risque d'entreprise (par exemple le potentiel impact direct sur la valorisation boursière). A quel moment la bascule peut-elle être faite entre le risque d'entreprise non assurable et celui qui est assurable ?

Les assureurs sont-ils prêts à aborder différemment l'assurance cyber à partir d'une valorisation des données intangibles ? Quels éléments leur permettraient-ils de mieux définir l'évaluation de l'exposition, de quelles informations de souscription vont-ils avoir besoin ? Est-il possible d'envisager une modélisation pour indemniser l'assuré pour ce genre de sinistre alors même que la modélisation des biens intangibles est encore à un stade exploratoire ?

Réunion5. Comment l'assurance et la réassurance peuvent-ils mettre cela en place ? Quelles seraient les informations nécessaires ? Comment se gérerait alors la souscription et les sinistres ? Peut-on penser que l'offre évoluera rapidement ? Quelles sont les informations nécessaires pour gérer un sinistre ?

Réunion6. Comment pourraient être mises en place les capacités financières à hauteur des enjeux financiers du risque cyber pour l'assurance et la réassurance afin que ce risque-là soit porté de manière crédible ? Comment rassembler des capacités pour que la couverture d'assurance puisse atteindre une taille critique justifiant le transfert de risque en cas de risque important ? Comment démontrer que des mesures de prévention ont-été mises en place ? Les captives – l'appel à des instruments financiers alternatifs – peuvent-elles répondre à ces enjeux ?

Dès lors que les scénarios de risque sont quantifiés et que leurs chiffres d'exposition financière sont crédibles dans le cadre d'une méthode validée par les auditeurs, il devient possible de remplir la matrice[4] en décomposant les scénarios en risques élémentaires auxquels sont associés des montants financiers constituant cette exposition totale. Retour sur la matrice des couvertures de risque année1.

Une fois la matrice renseignée par plusieurs scénarios, les risques élémentaires apparaitront comme partagés par divers scénarios montrant l'accumulation du risque.

Comment exploiter ces informations du point de vue statistique pour les assureurs et les réassureurs qui ont besoin de définir le périmètre de leur exposition et de tarifer ce risque de manière appropriée ?

Peut-on penser qu'une offre d'assurance cyber portant sur les intangibles puisse répondre à court terme aux besoins du *risk manager* pour un montant de garantie proposé adéquat ?

Réunion 7 conclusive : présentation des résultats, validation par les parties prenantes. Présentation du plan d'action pour la diffusion et la communication.

[4] Voir http://www.irt-systemx.fr/wp-content/uploads/2016/11/ISX-IC-EIC-transfert-risque.xlsx (version bilingue)

VI. INTRODUCTION

VI.1. Constat

La première année de la recherche a conduit à des avancées réelles : cinq recommandations et l'élaboration d'une matrice clarifiant l'offre cyber en matière d'assurance. Au-delà de ces recommandations ce travail a le mérite non quantifiable de réunir l'ensemble des acteurs de la chaine de valeurs de l'assurance. Les discussions permettent de faire bouger les lignes avec pour objectif l'intérêt général ainsi qu'une meilleure résilience de l'économie face à la survenance d'un acte cyber malveillant.

Depuis la publication du rapport, certaines recommandations ont été reprises par d'autres documents, ont fait déjà l'objet de mise en application ou font, désormais, l'objet de recherches approfondies. **Voir en annexe 10 le suivi des recommandations présentées dans le rapport année 1 (reprises dans l'annexe 9).**

La première année de la recherche a ainsi mis en évidence quels étaient les verrous du transfert du risque cyber vers l'assurance. Les travaux ont montré la validité de la méthode SPICE[5] qui permet au *Risk Manager* de maîtriser son exposition en quantifiant financièrement son risque cyber sur l'appui d'informations internes à l'entreprise. SPICE conserve tout son sens lorsque le chiffre financier final du scénario catastrophe cyber interne à l'entreprise est reconnu et validé par les parties prenantes de la valorisation des données intangibles de l'organisation. Est-ce que ces règles peuvent être agréées par les différents acteurs ?

Pour cette seconde année d'étude, n**ous faisons le constat qu'à court et moyen terme, l'assurance jouera un rôle de prescripteur d'outils de sécurité cyber pour les PME et TPME**. Néanmoins **cela sera plus délicat pour les grands groupes**. Actuellement, **les assureurs ne disposent pas de la totalité des éléments actuariels qui leurs sont nécessaires pour dimensionner leur offre cyber, notamment en ce qui concerne les données intangibles lesquelles ne font pas encore l'objet de qualification juridique ni de quantification financière et comptable.**

Ainsi, principalement dans les grandes entreprises, les décisions prises pour des investissements en cybersécurité découlent trop souvent d'autres arguments que les injonctions en provenance du marché de l'assurance.

Essentiellement pour les grands groupes, les offres assurancielles cyber ne sont que partiellement adaptées à leurs besoins d'accompagnement de leur transformation numérique si tant est que ces derniers soient compris et que leur exposition financière ait été définie en interne.

Au-delà de la compréhension de l'exposition au risque, les capacités financières à disposition des sociétés d'assurance ne permettent pas forcément de répondre aux demandes des grands groupes. Leurs réassureurs sont extrêmement vigilants sur les problématiques de cumuls et demandent un contrôle strict des engagements pris par les assureurs.

Malgré cela, la grande majorité des sociétés d'assurance qui interviennent sur le marché des risques d'entreprises en France ont développé, ces dernières années, des offres standard à destination des TPE/PME. Un marché de masse est en train de se structurer.

Nous proposons de poursuivre la réflexion en restant pragmatique et en reversant la proposition de la recherche conduite la première année. **L'approche demeure orientée *risk management* – la maîtrise en**

[5] Méthodologie SPICE https://www.lineon.fr/offres#vers-une-gouvernance-partagee-et-intelligente-du-risque-cyber

interne des éléments financiers constituant le risque cyber qui doit être traité comme un risque d'entreprise demeure primordiale mais il s'agit d'aider l'assurance à mieux connaître son appétit aux risques cyber en étudiant la valorisation des biens intangibles de l'organisation.

La transformation digitale de notre économie est un facteur de croissance et d'opportunité business ; il parait donc crédible de dire que la part intangible de l'entreprise va aller croissant. Plus une entreprise est digitalisée, plus elle est exposée à l'internet, plus sa surface d'attaque augmente. L'opportunité business doit s'accompagner d'une appréciation du risque cyber.

Nous émettons l'hypothèse que la valeur intangible constituera et constitue déjà pour nombre d'entreprise une part de plus en plus importante de leur valorisation. Auditeurs, administrateurs, investisseurs, actionnaires, commissaires aux comptes et agences de notation évaluent l'entreprise et concourent à sa valorisation. Tous vont bientôt demander aux entreprises de présenter, en toute transparence, les actions mises en œuvre pour protéger et valoriser le patrimoine informationnel de l'entreprise – ses données intangibles. Ils vont demander de démontrer la façon dont le risque sur les valeurs intangibles est géré. En retour, les conseils d'administration vont devoir expliquer quelle est la gouvernance qui a été mise en place pour gérer, non seulement le risque cyber sur un plan technique (et de conformité), **mais également sur le plan de sa gestion financière par le département de la finance et donc par le *risk manager***.

En retour, l'organisation va devoir faire la preuve de son respect des législations, des règlements, de la conformité mais également de son « efficience » quant à la gouvernance du risque cyber mise en place en son sein dans le cadre de ses efforts de transformation digitale. Quelle est sa résilience au risque digital. Elle va devoir, en effet, démontrer comment l'entreprise dans son concept d'entreprise étendue en lien avec tous ses partenaires, clients et fournisseurs (son écosystème) est résiliente. Comment elle a mis en place une gouvernance des données ainsi qu'une gouvernance du risque cyber.

Actuellement, la valorisation du patrimoine informationnel est laissée au marché car la valorisation des actifs immatériels est faite en bourse. L'immatériel et le *Good Will* qui valorisent les bénéfices futurs ne sont pas inscrits dans les bilans comptables.

Cependant, les auditeurs, les investisseurs, le régulateur et les agences de notation vont bientôt – si ils ne le font pas déjà, demander que soit mise en place, en interne, une politique de *risk management* dont une des missions sera de démontrer les moyens mis en place pour déterminer la valeur de l'exposition maximale au risque cyber et qu'elles ont été les mesures efficaces mises en place en terme de gouvernance du risque pour protéger au mieux le patrimoine informationnel et donc la valeur de l'organisation.

C'est là où se situe l'enjeu : **le conseil d'administration pourrait donner mandat au *risk manager*** d'orchestrer la réponse à ces deux questions en lien étroit avec les prescripteurs de sécurité en interne entreprise que sont les *Security Officers, les Product Security Officers,* la direction informatique en lien avec les responsables de la sécurité.

Par ce biais-là, le *risk manager* accentue et crédibilise encore plus son rôle d'interface unique de l'entreprise vis-à-vis de l'assurance pour déterminer quelles sont les conditions de couverture pertinentes pour son besoin. **Les assureurs ayant du mal à appréhender la valorisation intangible de l'entreprise. Ils ne sont donc pas reconnus comme un acteur clef de la protection de ces biens.**

VI.2. Objectifs de la recherche

Les travaux de recherche appliquée du séminaire année 2 s'attachent à déterminer ce que les auditeurs, les régulateurs et les agences de notations ont besoin pour valoriser les biens intangibles au regard du risque

cyber en l'absence d'inscription comptable de la donnée dans les livres de compte et en l'absence de traduction financière du retour sur investissement en matière de cybersécurité. Ils vont pouvoir dire ce dont ces derniers ont besoin pour comprendre le risque cyber afin qu'ils le traduisent dans les termes nécessaires à la valorisation. Quelles sont donc les conditions de la valorisation de la donnée – du bien intangible immatériel ?

Nous émettons l'hypothèse qu'interroger les acteurs en charge de la valorisation des biens intangibles profitera au marché de l'assurance et lui permettra d'aider à l'élaboration des éléments financiers constitutifs d'une analyse de risque financière du risque cyber.

Interroger ces acteurs sur leurs responsabilités concernant la prise en compte de la gouvernance du risque cyber qu'ils suivent apportera des éléments de compréhension supplémentaires.

Interroger ces acteurs sur les responsabilités des membres du Conseil d'administration vis-à-vis des investisseurs, auditeurs, commissaires aux comptes, des régulateurs, des agences de notation permettra de balayer les attendus actuels et à venir.

Quelle est l'utilité de cette recherche pour le marché de l'assurance ? **Le principe de l'assurance est de remettre l'assuré dans les conditions dans lesquelles il se trouvait avant le sinistre sans enrichissement induit**.

Aujourd'hui, en matière d'attaque cyber, malgré des progrès, les assurés peuvent se heurter à une contradiction entre ce principe et la nécessaire amélioration de leurs systèmes après sinistre. **La résilience ou l'anti-fragilité[6] réclament une situation améliorée après sinistre**. Ce qui contrevient au principe assuranciel. De plus, pour assurer des actifs immatériels, le contrat assurantiel bute sur l'absence de qualification et de quantification de la donnée. Les contrats d'assurance proposent essentiellement d'indemniser les mises en cause de la responsabilité de l'entreprise, les pertes d'exploitation, les pertes de profits futurs et proposent des services d'assistance pour limiter les pertes. Intéressant mais pas suffisant pour répondre aux besoins exprimés par les assurés.

Dans le cadre de ses contraintes métier, réglementaires et de solvabilité, l'assurance a pris en compte le transfert du risque cyber demandé par les entreprises. Ce transfert ne va pas aussi vite et aussi loin que le souhaiteraient principalement les grandes entreprises notamment dans la protection des biens intangibles et le financement de leur risque qui, aujourd'hui, font la richesse d'une entreprise (valorisation boursière). Ainsi, dans un monde de plus en plus digitalisé, les assureurs doivent accélérer leur compréhension du risque cyber afin de mieux accompagner le développement de l'économie numérique.

Jusqu'à présent, les assureurs se sont développés pour protéger les actifs tangibles : la responsabilité du fait des actifs. Ils ont besoin de connaître la qualification et la quantification de la donnée immatérielle ainsi que les conditions de la valorisation des biens intangibles. La matrice produite par le séminaire année1 montre la conséquence du risque cyber sur les actifs tangibles de l'organisation. Actuellement, le marché de l'assurance ne répond pas encore de façon adéquate au risque cyber pour ce qui est des dommages à la confiance – impacts sur les cours de bourse et les marchés futur, la réputation mais pas non plus sur la protection de la protection intellectuelle, le vol d'innovation et de R&D, les données d'ingénierie, les données personnelles et clients, le sabotage et l'espionnage. Le marché de l'assurance exclut de ses couvertures une bonne partie du patrimoine informationnel de l'entreprise lequel peut représenter jusqu'à 85% voire plus de la valorisation

[6] Nassim Nicholas TALEB, *Antifragile Les bienfaits du désordre*, https://www.lesbelleslettres.com/livre/80-antifragile

boursière. Or, les attendus de la croissance par la digitalisation de l'entreprise concernent avant tout ces éléments.

Afin de dimensionner leur offre cyber, les assureurs ont notamment besoin d'avancer sur trois thèmes : la quantification du risque cyber des biens intangibles au sein des organisations pour déterminer leur exposition au risque, **comprendre comment va s'organiser la gouvernance du risque cyber** et **quels en sont les attendus par les acteurs de la valorisation de l'entreprise**.

L'organisation va être interpellée sur sa politique de gouvernance des données, de cybersécurité et de *risk management*. Elle va devoir répondre de son niveau de maturité et de résilience. Les questions qui seront posées seront les suivantes : quelle est votre identification à votre exposition au risque ? Quelles sont les mesures de prévention que vous avez mises en place ? Quels sont vos indicateurs, vos métriques, vos mesures d'impact ? Pouvez-vous démontrer que vous avez pris les bonnes décisions en matière de sécurité au regard de vos objectifs business dans le respect de la loi et des règles de conformité ?

Les interlocuteurs vont faire le lien entre la valeur de la société, la gouvernance de l'entreprise et le lien avec l'impact sur le business du risque cyber. Il s'agira de pouvoir faire la démonstration que les mesures prises sont efficaces en termes de protection et que la prise de risque est éclairée. La décision de développer de nouveaux services en internes et en externe, les nouvelles applications et l'automatisation doit être prise en prenant la mesure (quantifiée financièrement) des risques supplémentaires que cela implique. Il s'agira également de démontrer que des mesures ont été mises en face de politiques de prévention et de confiance. **Tous ses éléments font partie d'une gouvernance d'entreprise résiliente**.

VII. La Prise en compte du risque cyber par les agences de notation financière

Verrous

La prise en compte du risque cyber dans la définition de la note de l'entreprise et dans sa qualité de crédit.

Les agences de notation intègrent-elles désormais le risque cyber et valorisent-elles les données intangibles ? Quelle est la valorisation du *Good Will* ?

Comment valoriser l'intangible à l'appui de la transformation digitale dont les résultats, les opportunités et revenus attendus vont être un élément prospectif ?

VII.1. *Considerations on Cyber Risk* : perception et prise en compte du risque cyber[7]

A.M. Best[8] est une agence spécialisée dans l'évaluation des sociétés d'assurance et de réassurance. Elle produit des notations, des analyses sur la capacité de crédit, des informations spécifiques contenues dans des rapports ainsi que des commentaires publiés.

VII.1.a. Le risque cyber se situe désormais en haut des agendas des compagnies d'assurance et de réassurance

- **Un risque majeur …**

Jusqu'à présent, le risque cyber était pris en compte pour les entreprises pour lesquelles l'importance du numérique était majeure. **L'évolution de la digitalisation modifie l'ordre des priorités** : la cartographie produite par *Allianz* en 2016 place le risque cyber en haut de la liste (3e au niveau mondial) ; le Royaume-Uni et l'Allemagne le positionnent comme le *top business risk*; une étude des Lloyds de fin 2016[9] indique que plus que 90% des personnes ayant répondu à l'enquête avaient déclaré avoir été victimes d'une attaque. L'étude de terrain de l'IRT SYSTEMX confirme l'ampleur des attaques[10].

La réglementation évolue. La législation américaine (NY) en date de janvier 2017 impose d'apporter des réponses adéquates en cas de *data breach*[11]. L'entrée en vigueur du RGPD européen en mai 2018[12] impose également des règles plus contraignantes en matière de prise en compte du risque cyber au regard de la protection des données personnelles.

---

[7] Présentation par *A.M. Best*

[8] http://www.ambest.com

[9] A report by Lloyds', « *Facing the Cyber Risk Challenge* », 20th September 2016, 22 pages.

[10] Les cyberattaques et leurs préjudices sur les entreprises : quantification et qualification, https://www.irt-systemx.fr/wp-content/uploads/2017/10/ISX-IC-Cyber-Risque.pdf

[11] Best's Briefing, US Cyber Risk, « *A.M. Best comments on New York States New and Revised Regulation on Cybersecurity* », Regulatory Review, February 17th 2017

[12] En mai 2018, est entré en vigueur le règlement général de l'Union européenne sur la protection des données personnelles (RGPD).

La réputation des entreprises est directement impactée comme l'ont montré les attaques cyber qui ont fait l'objet d'une médiatisation ex. Yahoo[13], Banque Centrale du Bengladesh[14].

… et devient une opportunité business pour les compagnies d'assurance et de réassurance.

Par rebond, ces évènements impactent les organisations qui veulent couvrir le risque. Ce dernier représente également une opportunité de business telle qu'exprimée **fin janvier 2017 lors de Paris Fin-Tech**. **Le régulateur, des représentants de l'Assurance et de la Réassurance ont ainsi exprimé leur volonté de soutenir la croissance de l'économie digitale directement** en tant qu'opérateur de données sensibles **et indirectement en tant que porteur de risque**. François Villeroy de Galhau, gouverneur de la banque de France, a ainsi déclaré : « ***avec l'aide des réassureurs, les assureurs doivent être en mesure de répondre aux besoin de couverture contre les cyber-risques, une préoccupation qui touche l'ensemble des entreprises des plus petites aux plus grandes*** » ; « ***les entreprises d'assurance peuvent et doivent se nourrir de leur propre expérience contre les cyber-risques pour faire émerger une offre française et européenne de cyber assurance plus mature*** ».

VII.1.b. Intégration du risque cyber dans la notation

- **Prendre en compte le caractère complexe du risque cyber**

ISACA IT Risk Framework[15] définit le risque cyber ainsi : « the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise ».

Le risque cyber s'étend et mute au rythme de la technologie. Difficile à modéliser et à monitorer, il **peut être perçu comme une taxe additionnelle sur l'innovation** ; il peut être à la fois la conséquence d'une erreur non malveillante (technique et humaine) et également malveillante (espionnage, cyber crime, sabotage, terrorisme).

Il existe un problème de définition dans l'industrie : les termes décrivent des éléments différents. Ce manque d'accord sur les termes importants **constitue un problème entre assureurs et réassureurs**. L'industrie et les opérateurs sont encouragés à partager un langage commun.

De même, **la question des *silent covers* (couvertures silencieuses) doit être éclaircie par l'assurance et la réassurance**. Le constat est qu'aujourd'hui, un consensus fait défaut sur nombre de points importants.

- **Un grand nombre de données touchées, un véritable défi**

Les pertes et les dommages couvrent de très nombreux domaines : le vol de propriété intellectuelle et d'informations commerciales sensibles ; l'interruption et la distorsion de business ; l'extorsion ; la fraude ; les atteintes aux données personnelles ; les atteintes aux infrastructures ; la perte de réputation ; les dommages physiques – sur les personnes et le matériel ainsi que le coût des réponses et des investigations.

[13] Yahoo a fait l'objet d'une attaque cyber sur 3 milliards de ses comptes en 2013. Voir https://www.sec.gov/news/press-release/2018-71

[14] La Banque centrale du Bengladesh a fait l'objet, en février 2016, d'une attaque informatique, 81 millions de dollars ont été dérobés.

[15] https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx

VII.1.c. L'approche d'A.M. Best dans sa prise en compte du risque cyber pour l'exercice de notation

- **Les éléments constitutifs de la décision de notation – méthodologie générale**

Trois éléments principaux se conjuguent pour définir la solidité financière de la compagnie d'assurance : la force bilancielle (*Balance Sheet Strength*), la performance opérationnelle (*Operating Performance*) et le profil de marché (*Business Profil*e). Ces derniers se combinent avec l'*Entreprise Risk Management* et le risque pays. La décision de notation est une combinatoire de ces éléments.

- **La décision de notation face aux risques cyber**

Le *risk management* est le fil conducteur entre des éléments d'analyse qui sont la force bilancielle, la performance opérationnelle et le profil de marché.

L'appréciation du risque cyber d'un assureur ou d'un réassureur s'effectue à deux niveaux :

- en tant qu'acheteur – interne : l'organisme détient des données personnelles sensibles pouvant être sujettes à des attaques. La compagnie peut alors choisir de couvrir son risque interne en achetant une solution d'assurance ou de réassurance. Il s'agit, pour *A.M. Best*, de comprendre le travail fait par le *risk management* de la compagnie en interne pour identifier, mesurer, vérifier qu'elle est apte à répondre à ce risque cyber en interne.
- en tant que vendeur – externe : la compagnie peut fournir une solution de risque cyber à ses clients. L'étude d'*A.M. Best* porte, dans ce cas, sur les couvertures offertes par la compagnie qu'elles soient directes ou indirectes.

Sur la partie interne, l'agence demande aux sociétés qu'elle note comment elles identifient leur risque, comment elles le quantifient et mitigent leur exposition. **Le *risk management* porte sur la qualité de la fonction, le monitoring des risques et la gouvernance associée** – existe-t-il un *risk committee* ?, un organe dédié ?, quelle est la fréquence des réunions ?… L'appréciation porte sur le fait de savoir si le *risk management* est intégré dans l'entreprise.

Sur la partie externe, l'agence interroge le niveau d'exposition au risque cyber connu ou pas lié à la souscription. La question est alors de mesurer l'exposition au risque cyber en tant que fournisseur de service financier – souscripteur. La compagnie doit, dans ce cadre, démontrer sa capacité à manager son risque ; **présenter** – articuler sur son exposition au risque cyber qui dérive de ses activités de souscription ; **démontrer** où se situe le risque cyber connu ou silencieux au sein des polices d'assurance – *Property, D&O – Liability*, *Business Interruption*, *Cyber Extortion* et *Loss – Data Corruption*. **La performance technique de la compagnie est analysée par lignes de business**. Enfin, des questions sont posées sur la capacité de l'entreprise à identifier, mesurer et contrôler son exposition générale au risque cyber.

Dans un cas comme dans l'autre – l'exposition au risque cyber interne et externe, le *risk management* est considéré comme influençant les trois grands éléments d'analyse : le *Balance Sheet Strength*, l'*Operating Performance* et le *Market profile*.

Les notations sont prospectives et l'horizon temporel typique est de trois ans.

- **La prise en compte du risque cyber est-elle posée dans la présentation des business plans ?**

Le **SRQ** – *Supplementary Rating Questionnaire* (outil *A.M. Best*) interroge le risque cyber sur les expositions qui découlent des risques souscrits, le niveau de couverture du risque cyber dans les couvertures cyber *stand alone* ou en tant que sous limite au sein des autres polices. Quelles sont les lignes de business concernées ; le

niveau de protection cyber acquis par l'entreprise ? Cette information est utilisée dans le cadre de l'analyse de la partie *risk management* de l'entreprise.

Une telle question peut être posée de manière générale au management lors du meeting annuel sur les aspects internes (victimes de risque cyber) et externes (et fournisseur de protection cyber).

- **Est-il demandé que le SMP (le calcul du sinistre maximum possible) prenne en compte le risque cyber ?**

Il n'est pas demandé actuellement aux compagnies d'assurance et de réassurance si elles intègrent dans leur SMP le risque cyber. Cela pourrait être le cas à l'avenir et l'utilisation de scénarios catastrophe pourrait être une piste sur le modèle de ce qui se fait pour les catastrophes naturelles.

- **Les outils utilisés par *A.M. Best* concernant l'appréciation du risque cyber pour le risque cyber interne et par le *risk management* des compagnies**

Il est fait part de l'utilisation de la solution de *Cyence, Inc. – security score card*[16].

Un questionnaire cyber dédié. Quel est le régime de risque management déployé dans l'entreprise ; quelles sont les configurations de sécurité mises en place ; quel est le niveau de sécurité des réseaux ; qui détient et manage les droits des comptes à privilèges ; quel est le niveau d'éducation et d'*awareness* des utilisateurs ; comment s'organise la réponse à l'incident – gestion de la crise ; quelle est la politique mise en place pour se protéger des *malwares* ; enfin comment s'organise le monitoring ; quelle sécurité mise en place dans les pratiques de télétravail.

Pour *A.M. Best*, la non prise en compte du risque cyber n'est pas une option et **l'ERM (Entreprise *Risk Management*) doit être en mesure d'identifier les stratégies pour traiter le risque cyber résiduel** si tant est que l'ERM arrive à définir son exposition au risque cyber afin de préparer son transfert vers l'assurance. L'analyste s'attache à identifier les couvertures, les limites et les responsabilités dans chaque programme.

A.M. Best se fonde également sur le résultat des **échanges annuels avec le management**.

- **Les challenges posés par le risque cyber externe lié aux activités de souscription**

Le risque cyber est difficile à modéliser par manque de données historiques, à cause du nombre réduit de données disponibles et de leur piètre qualité pour celles qui existent. Le fait que les entreprises ignorent souvent qu'elles ont fait l'objet d'attaques, qu'elles refusent de communiquer pour des raisons légales ou de réputation et que la technologie dans ce domaine évolue très vite rendent le ***pricing* de la souscription compliqué**. L'absence de frontière géographique, de périmètre du risque pose question quant au **phénomène d'agrégation**.

Les corrélations globales donnent un caractère systémique au risque cyber. Le ***wording* des polices et les *silent covers* surajoutent à la complexité**. La question du cumul se pose également avec acuité. Que ce soit en Europe continentale ou dans les polices cybers anglo-saxonnes (qui sont souvent dédiées), la question de l'agrégation des risques cyber se pose pareillement. Or, *A.M. Best* doit comprendre comment la compagnie gère son risque et contrôle son exposition : comment le cumul est calculé et validé.

Selon l'agence, ces éléments conduisent à **des prises de position conservatrices sur le marché**, une frilosité de la part du marché européen continental. La souscription ne dispose que de très peu d'informations, ou ces dernières sont exprimées de façon trop prudente. De manière générale, les réassureurs offrant des

[16] Voir https://www.cyence.net/

couvertures de risque cyber le font sur des engagements limités. Le marché américain est plus mature ayant débuté il y a dix ans.

- **Le Cloud et l'assurance CBI – *Contingent Business Interruption***

L'exemple de **l'assurance *CIB*[17] pour le *Cloud computing*** est mis en exergue. Les avantages et les opportunités pour le business des solutions cloud sont nombreux. L'assurance *CBI* va couvrir l'assuré en cas de dommage physique ou de perte de *Dependent Property* (une propriété opérée par d'autres sur laquelle on dépend pour délivrer des matériaux et des services, accepter des produits et des services et ou fabriquer des produits qui doivent être livrés à la compagne – sous-traitance). Or, le Cloud rentre dans le champ de cette définition de *Dependent Property*. Ceci implique que, bien que de manière générale l'on puisse penser que la perte de données électroniques ne soit pas couverte par le cloud, **le juge détient une forte capacité d'interprétation**. Ainsi, **la jurisprudence donne une interprétation plus large des dommages physiques pour y inclure la corruption, la perte des données ainsi que l'interruption de service et la perte d'accès, d'usage et de fonctionnalité**.

- **Le risque d'accumulation**

Concernant les couvertures silencieuses, l'autorité de contrôle britannique a pris l'action de les identifier pour les éliminer. Les assureurs et les réassureurs ont été enjoints de conduire un travail important en interne pour parcourir leurs polices pour identifier les expositions au risque cyber qui ne sont pas a priori identifiées comme telles. Le risque d'accumulation du risque cyber est d'autant plus important qu'il peut avoir une source cyber et affecter des polices cyber dédiées ou des lignes traditionnelles (de type *Property*), non cyber et affecter des polices cyber non dédiées (type perte de support présentant des données sensibles comme les clefs USB, ordinateurs portables etc.) ou affecter directement l'assureur, le réassureur et les assurés (cyber attaque sur un assureur et ses clients en même temps).

VII.1.d. Le risque cyber et la notation des entreprises d'assurance : les prochaines étapes

- **Développer la modélisation**

Les études actuarielles font encore défaut et les modèles de risque cyber ne sont pas encore matures. La modélisation de l'exposition au risque demeure un véritable défi. Comment modéliser le SMP ?

Une fois que les modèles seront développés, le but pourrait être d'intégrer le risque cyber dans l'analyse générale de notation de la même façon que le sont les expositions aux catastrophes plus traditionnelles.

Compte tenu de **l'état de l'art en la matière, les modèles et leurs *outputs* peuvent varier en fonction des paramètres retenus et de la qualité des données utilisées**. Deux points demeurent importants : **les modèles utilisés doivent être pertinents** et **les *outputs* compris** ; **l'utilisation des modèles doit être justifiée**.

[17] Assurance qui couvre les pertes financières provoquées par un dommage matériel suite à une interruption d'activité.

VII.2. Comment les risques cyber sont-ils pris en compte et peuvent influencer la notation d'une organisation ?[18]

***Moody's* est une agence de notation centenaire**, notant tout type d'entités financières et non financières, des États et des collectivités territoriales – principalement aux États-Unis[19].

VII.2.a. Présentation de l'organisation

La raison sociale d'une agence de notation est de **noter le risque de crédit**, c'est-à-dire d'évaluer la **capacité d'un emprunteur à rembourser sa dette**. La notation correspond à une espérance de perte – la probabilité de défaut et la perte en cas de défaut. L'échelle de notation est composée de vingt-trois niveaux, du Aaa (« triple A ») au C.

L'agence publie également **des commentaires** en cas d'évènement affectant la notation ou plus généralement affectant la qualité de crédit d'une entreprise – la qualité de crédit est une notion moins normée que la notation : un évènement peut avoir un impact positif ou négatif sur la qualité de crédit d'une entreprise sans pour autant affecter la notation de l'entreprise.

En cas de changement de notation, un communiqué de presse est publié. La publication d'une notation est accompagnée **d'un document « *credit opinion* »** expliquant pourquoi l'agence a attribué cette notation. Ce document est mis à jour périodiquement (par exemple tous les six mois) et à chaque changement de notation.

Une notation n'est pas une recommandation mais une opinion.

Des rapports sont également publiés par secteur d'activité pour discuter les tendances à l'œuvre dans ce secteur et les perspectives du secteur.

Lorsque certains thèmes affectent plusieurs secteurs d'activité, **des rapports « *cross sectors* »** sont également publiés. Par exemple, en 2015, Moody's a publié un document discutant de l'exposition de l'ensemble des secteurs d'activités au risque cyber[20].

VII.2.b. Présentation générale des méthodes de notation

Les éléments principaux de notation pour les entreprises s'organisent selon **une approche *top down*** dans laquelle est prise en compte le secteur industriel dans lequel l'entreprise évolue, et les tendances à l'œuvre dans ce secteur, les parts de marchés de l'entreprise, la diversification de son activité, ses produits, et divers ratios financiers. **Sont également prises en compte la stratégie de l'entreprise et son organisation**.

La méthodologie est appliquée **par secteur industriel**. Chaque entreprise est analysée au travers d'**une grille**, ou *score card*, qui se divise pour partie entre une appréciation financière – ratios (profitabilité, levier financier, couverture de la charge d'intérêt, …) et **pour partie sur une appréciation plus qualitative** (positionnement, profil de risque…).

Les différents facteurs de la *score card* font l'objet d'une analyse objective donnant lieu à un score – établi selon un benchmark, et une pondération est affectée à chacun de ces facteurs pour obtenir la note finale.

---

[18] Présentation par *Moody's*.
[19] https://www.moodys.com
[20] Moody's Investor Service, Sector in Depth – Cross Sector Global, «*Cyber Risk of Growing Importance to Credit Analysis*», 9 pages, 23rd November 2015.

Au-delà de l'analyse objective et quantitative, **la qualité du management est également appréciée** selon les termes suivants qui ont la capacité d'influer sur les résultats financiers – la gouvernance d'entreprise, la transparence, les contrôles internes. **Le risque de survenance d'évènement exceptionnel** « » est également pris en compte en analysant l'impact de scénarios de stress. L'un de ces événements exceptionnels peut être une attaque cyber.

VII.2.c. Les éléments intangibles pris en compte à ce jour par Moody's

Les actifs intangibles, tels que la réputation, sont intégrés dans l'analyse. Par exemple, dans le cas de Volkswagen à la suite du scandale des émissions polluantes *Dieselgate* de 2015, les analystes ont cherché à évaluer quel pourrait être le coût supplémentaire à court terme du rappel des véhicules et quelles pourraient être les conséquences financières des poursuites judiciaires, mais aussi quelles pourraient être les conséquences sur la réputation de l'entreprise. Une évaluation des conséquences futures sur l'activité de l'entreprise a également été conduite.

VII.2.d. Focus sur le risque cyber

L'agence est amenée à commenter les impacts du risque cyber sur les notations des sociétés d'assurance et des entreprises[21].

L'agence a publié de nombreux commentaires suite à des attaques cyber. Par exemple, lorsque *Sony* a été victime d'une attaque en 2011, *Moody's* a publié un commentaire expliquant pourquoi cette attaque avait un impact négatif sur la qualité de crédit de l'entreprise. L'analyse prenait en compte les éléments suivants : **la hausse des coûts financiers**, **l'impact sur la réputation** et **le risque de baisse des parts de marché**. D'autres exemples sont présentés plus loin.

De façon générale **a posteriori**, les conséquences de l'attaque sont appréciées en fonction de ses impacts financiers – **les coûts supplémentaires pour faire face aux conséquences de l'attaque peuvent faire baisser la rentabilité**, mais aussi en fonction d'impacts plus qualitatifs – **chute des revenus**, du **nombre de clients** et la **réputation**. Différents facteurs de la *score card* peuvent donc être affectés. L'agence peut ainsi mesurer l'impact global sur la notation ou sur la qualité de crédit de l'entreprise victime de l'attaque.

Mais **le risque cyber est également analysé a priori**. Il est directement pris en compte dans certaines méthodologies pour les secteurs particulièrement à risque.

Dans les autres cas, **le *cyber risk* est analysé au même titre que les autres événements de nature exceptionnelle** qui peuvent impacter la qualité de crédit d'une entreprise – comme le risque catastrophes naturelles par exemple, il est intégré **dans l'analyse de l'*event risk*** : en plus du scénario central sur lequel repose les scores des différents facteurs en règle générale, **des scénarios de stress sont évalués**. Si l'impact de ces stress qui est évalué au travers des ratios financiers et des facteurs qualitatifs utilisés dans la *score card* est trop significatif – un risque de dégradation de la notation de plus de trois crans, la notation doit être ajustée pour refléter ce risque. L'agence souhaite, en effet, limiter le risque de transition trop importante dans les notations et s'assure que la notation, après scénario de stress, n'est pas très éloignée de la notation avant le stress.

[21] Moody's Investor Service, Sector in Depth, Cross Sector Global « *Cyber Risk of Growing Importance to Credit Analysis* », 23rd November 2015.

Le **risque cyber ne fait pas l'objet d'une modélisation explicite en tant que telle**, mais il est un risque parmi d'autres pouvant impacter la notation et dont la prise en compte va aller croissant.

À ce titre, le document de l'agence publié en février 2015[22] constate que le risque cyber devient de plus en plus important pour un grand nombre de sociétés et, en conséquence, **ce risque va être amené à être de plus en plus pris en compte**. Plus dans certains secteurs que d'autres – la Finance avec un focus sur les chambres de compensation sur lesquelles le risque cyber fait peser un risque systémique car les *Clearing Houses* ont un rôle d'infrastructure dans le système financier[23] ; les assurances[24] sont mentionnées mais pas encore clairement identifiées comme étant à très haut risque comme le secteur bancaire.

La logique d'appréciation de l'agence s'est construite par l'analogie que fait peser le risque cyber sur les *Utilities* – le secteur des infrastructures. D'ailleurs, de nombreux commentaires ont été publiés pour ce secteur d'activité.

- **Les sources à disposition de l'agence pour apprécier le risque, a fortiori le risque cyber**

Des discussions ont lieu au moins une fois par an **entre l'agence de notation et le top management** pour interroger les membres exécutifs des conseils d'administration qui sont interrogés et challengés. Ces discussions incluent de plus en en plus le risque cyber – exposition au risque, mesures mises en place pour y faire face. **Les discussions sont recoupées avec les éléments disponibles, notamment les comptes publiés par l'entreprise**.

Une liste de sources est considérée comme sources fiables, mais il existe aujourd'hui peu d'éléments publics permettant d'apprécier l'exposition au risque cyber d'une entreprise.

- **L'appréciation du risque cyber au regard des mesures techniques – gestion opérationnelle**

Dans la plupart de cas, l'agence de notation considère que les sociétés qu'elle note et qui émettent de la dette – qui sont généralement les plus grandes sociétés – mettent en place le dispositif nécessaire – **plans et systèmes de défense**. Ceci est vérifié au travers d'échanges avec les entreprises notées. Si ces éléments sont effectivement mis en place, la note n'est pas affectée. S'ils font défaut, ceci peut avoir un impact négatif sur la notation.

- **L'appréciation du risque cyber au regard de la mise en place d'une gouvernance du risque cyber dans l'entreprise**

L'agence ne prend **pas en compte à l'heure actuelle la question de la gouvernance du risque cyber dans le sens du *risk manager***. Comme ci-dessus, son postulat est que la société dispose d'un *risk manager*.

- **L'appréciation du risque cyber au regard de l'évolution du cadre légal, réglementaire et des mesures de conformité**

Dans son document en date du 26 janvier 2016[25], **l'agence indique qu'elle continuera à évaluer dans quelle mesure les entreprises continuent de développer une « culture de défense » face au risque cyber**. L'agence s'attend à ce que les sociétés ne fassent pas seulement ce qui est attendu d'elles au regard des dispositions réglementaires, légales et de conformité compte tenu de la nature évolutive de la menace cyber. **Le**

[22] Voir note 3.
[23] Moody's Investor Service, Rating Methodology, « *Clearing House* », 7th January 2016, 44 pages.
[24] Moody's Investor Service, Sector in Depth, « *Cyber Insurance: High Risk Product with Potential to grow* », 19th November 2015, 14 pages.
[25] Moody's Investor Service, Sector Comment, « US Regulator Approves Cybersecurity Standards, a credit positive for Regulated Utilities », 28th January 2016, 3 pages.

règlement, la disposition légale deviennent ainsi un risque si les sociétés ne font qu'adhérer à une culture de conformité.

- **Évolution de l'appréciation du risque par Moody's**

Moody's est amené à **prendre de plus en plus explicitement le risque cyber dans ses analyses**. Dans le secteur des assurances par exemple, une enquête spécifique est effectuée sur la gestion du risque cyber par les entreprises. Les résultats de cette enquête – effectuée auprès d'assureurs américains et canadiens ont été publiés en février 2017[26]. Un document similaire a été publié sur le secteur bancaire en juillet 2016. **Les résultats de cette enquête montrent que cette question est de plus en plus prise en compte dans les rapports journaliers destinés aux risques managers et dans ceux mensuels présentés au Conseils d'administration**. La tendance montre une évolution dans la prise de conscience du top management.

VII.2.e. Les principaux cas d'attaque cyber qui ont fait l'objet d'un commentaire

- **Commentaire de l'attaque cyber dont a fait l'objet *Sony* en 2011[27]**

Moody's a considéré que cette attaque avait **un impact négatif sur la qualité de crédit de *Sony***, sans que la note soit modifiée[28]. Dans le premier commentaire, l'agence émettait un avis basé sur **la perte de confiance des clients**, et dans le second **l'impact du coût juridique**, **de la remise en état** et **des compensations offertes** aux clients qui subissaient une utilisation frauduleuse de leurs cartes de crédits. Selon l'agence, la réputation de l'entreprise n'était néanmoins pas à risque. Moody's a souligné de façon positive la réaction de *Sony* qui avait offert à ses clients abusés une assurance, ces derniers ayant bien réagi en retour. Un troisième commentaire en juillet de la même année revient sur l'impact de l'attaque cyber couplée avec les suites d'un tremblement de terre et s'inquiète de la capacité de l'entreprise à restaurer sa profitabilité[29].

- **Commentaires dans le secteur du *retail*, *Target* 2013, *Home Depot* 2014 et *WalMart* 2016**

En 2013, l'agence a jugé qu'une attaque cyber dont avait été victime ***Target*** **a eu un impact négatif sur la qualité de crédit de l'entreprise**, mais n'a pas modifié la note de l'entreprise[30]. *Moody's* insiste sur l**e coût financier à long terme** des conséquences juridiques et de la perte de confiance de la part des clients.

En 2014, le commentaire publié concernant ***Home Depot*** faisait référence aux évènements survenus un an plus tôt à l'encontre de Target en faisant référence **au coût de l'attaque**. L'analyse de *Moody's* de 2014 a ainsi pris en compte les enseignements de l'attaque survenue en 2013 sur une autre entreprise.

En 2016, un commentaire comparant la qualité de crédit de ***WalMart*** et de ***Target*** faisait une nouvelle fois mention de l'attaque de 2013 contre ***Target***[31] en mettant en exergue, **les conséquences qu'avait eu l'attaque sur la stratégie de l'entreprise** depuis cette date. Le document d'octobre 2016 montrait les répercussions de l'incident cyber à long terme sur la stratégie et **la réputation de l'entreprise**. Certes d'autres éléments

---

[26] Moody's Investor Service, Sector in-Depth, US and Canada Survey « *North American Insurers Step up Cyber Security Initiatives* », 9 pages.
[27] Moody's Investor Service, Investor Service, Issuer Comment, « *PlayStation Security Breach is Credit negative for Sony* », 2nd May 2011, 3 pages.
[28] Moody's Investor Service, Issuer Comment, « *Sony's Second Hack Attack and Security Breach are Credit negative* », 9th May, 2011, 3 pages.
[29] Moody's Investor Service, Investor Service, Global Credit Research, Announcement, « *Moody's sees slow recovery in Sony's profitability as a concern* », 11th July 2011, 3 pages.
[30] Moody's Investor Service, Global Credit Research, Issuer Comment, « *Target's, Credit Card Security Breach us Credit Negative for Company* », 19th December 2013.
[31] Moody's Investor Service, Issuer in Depth, « *Wal Mart Stores, Inc. and Target Corporation* », October 4th 2016, 6 pages.

rentraient en cause, **mais le lien entre attaque cyber et perte d'opportunité (actif intangible) sur des éléments attendus a été fait**.

- **Commentaires sur la société *USIS – Groupe Altegrity***

En 2014 au mois d'octobre, la société *USIS* a été victime d'une attaque cyber et d'un vol de données. Ses clients étaient peu nombreux et étaient principalement des agences fédérales américaines. Dans son appréciation, publiée au mois d'août de la même année[32], ***Moody's* estimait que la société pouvait absorber le risque cyber mais que sa note pourrait être modifiée en cas de pertes de clients**. La concentration des clients était un risque en soi, qui était reflété dans la faible notation de l'entreprise. **Il s'est avéré que les agences fédérales se sont détournées de de l'entreprise** à la suite de l'attaque. ***Moody*'s a dégradé sa note**[33]. L'entreprise a fait défaut. **L'attaque cyber a été responsable de la dégradation de la note et de la mise en défaut de paiement de la société.**

VII.2.f. La prise en compte par Moody's du risque d'accumulation

Comment une agence de notation peut-elle prendre en compte le risque d'accumulation d'un *Service Cloud Provider* comme *Amazon* ? Le phénomène d'intégration est exceptionnel mais réel.

Comment évaluer l'appréciation du risque cyber au regard des stratégies de digitalisation des entreprises ?

La **transformation digitale** représente à la fois des opportunités et risques pour les entreprises, en multipliant notamment les surfaces possibles d'attaque. **Cette question est de plus en plus prise en compte** dans l'analyse de certaines sociétés notamment pour les banques et les assurances[34] et une évaluation des mesures et des plans mis en œuvre par les entreprises est de plus en plus systématique. **Pour le moment, le risque cyber est essentiellement analysé en tant qu'*event risk* –** difficile de chiffrer a priori la survenance de l'événement, mais une analyse des conséquences en cas de réalisation de stress peut être menée.

VII.2.g. Appréciation du rôle des États face au risque cyber

Dans le secteur des ***Utilities*** notamment les infrastructures « vitales », ***Moody's* considère que l'État sera amené à soutenir l'activité des entreprises**[35] de ce secteur compte tenu de leur importance pour la continuité de l'activité du pays[36]. Cette appréciation a une conséquence sur l'appréciation du risque de défaut de l'entreprise en cas d'attaque cyber – le support de l'État pourrait contribuer à diminuer le risque de défaut. Dans une publication de 2012[37], *Moody's* fait ainsi référence à l'ouragan Sandy survenu dans les états de New York, du New Jersey et du Connecticut. Les autorités se sont porté soutien des entreprises de ce secteur.

---

[32] Moody's Investor Service, Investor Service, Global Credit Research, « *USIS security breach is credit negative for Altegrity ; no impact on rating if federal agencies restore business in short term* », 11th August 2014.
[33] Moody's Investor Service, Global Credit Research, Rating Action, « *Moody's Downgrade Altegrity CFR to Caa3, outlook negative* », 12th September 2014.
[34] Moody's Investor Service, Sector in Depth – Bank US « *Survey: Bank Boards Engage Growing Cyber Threat, Employ Security – Solutions Vendors* », 13th July 2016, 12 pages.
[35] Moody's Investor Service, Sector in Depth, « *In a major Cyber Attack the Likelihood of Government relief is High* », 15th October 2015, 9 pages.
[36] Moody's Investor Service, Sector Comment, « *US Regulator Approves Cybersecurity Standards, a credit positive for Regulated Utilities* », 28th January 2016, 3 pages.
[37] Moody's Investors Service, Sector Comment «*Utilities Remain Vulnerable and Attractive Target of Cyber Attacks, a Credit Negative* », 9 January 2017.

VII.2.h. La tendance de la prise en compte du risque cyber

Le risque cyber est désormais incontournable, **les méthodologies** pour sa prise en compte **vont encore évoluer**, **le benchmark des sociétés va se développer**.

Les entreprises seront de plus en plus challengées sur les impacts des risques sur leur situation financière et leur capacité de crédit. L'analyse pourrait de plus en plus prendre en compte des évènements prospectifs.

Une note pourrait-elle être dégradée pour un défaut de *risk management* cyber non pris en compte ? **Le *risk management* pourrait être intégré à la *score card* directement par un calcul par rapport à des ratios passés**. Des ajustements de la *score card* pourraient également avoir lieu **en fonction d'une vision prospective**.

Le **risk management pourra être apprécié de façon qualitative par des éléments culturels**, un *trade record*. **Les éléments quantitatifs pourront être amenés par la quantification des scénarios catastrophe développés en interne par l'organisation et par le montant des sanctions prévues en cas de non-respect**. Enfin, la preuve de la conformité aux règlementations et normes est nécessaire mais pas suffisante. La normalisation et la compliance deviennent un risque pour la réponse à apporter à la gestion du risque cyber.

VIII. La responsabilité des dirigeants face au risque cyber

Verrous

Quelles sont les responsabilités des Conseils d'administration (cadre réglementaire actuel et à venir – quelle évolution de la conformité) ?

Hors du cadre législatif ou réglementaire, quelles sont les responsabilités ou les risques encourus pour les mandataires sociaux ? Que demandent les actionnaires au regard de la digitalisation. Comment perçoivent-ils le risque numérique ? Les membres des conseils d'administration vont-ils devoir justifier de leur bonne gestion – d'une gestion efficiente en termes de gouvernance d'entreprise ?

VIII.1. La responsabilité des dirigeants face au risque cyber, le cadre légal et réglementaire[38]

Au vu de l'évolution du cadre juridique et réglementaire, le risque cyber doit être au cœur des préoccupations des dirigeants. On assiste à une recrudescence des cyberattaques qui pourrait être amplifiée par la protection des lanceurs d'alerte encadrée par la Loi pour une République numérique (« Hackers blancs »)[39] . Ces attaques pourraient avoir pour objet un détournement d'innovation et de R&D, un vol de données sensibles et stratégiques ou une atteinte à la vie privée. Elles pourraient avoir un impact sur la confiance, entrainer des actions de groupes[40], générer une atteinte à la réputation et des pertes financières (notamment chute du cours de bourse, etc.).

L'évolution du cadre légal et réglementaire dans son ensemble [Loi informatique et liberté (LI&L), le RGPD, la directive NIS, le directive sur le secret des affaires, la loi pour une République numérique, les délibérations de la CNIL et des régulateurs tels que l'AMF va dans le sens de l'exercice de nouvelles obligations par les dirigeants de l'entreprise face au risque cyber. **Un nouveau paradigme se met en place : les dirigeants vont être appelés à établir la preuve qu'une gouvernance du risque cyber a été mise en place au sein de leur organisation**.

VIII.1.a. Focus sur le cadre légal en matière de protection des données à caractère personnel (LI&L)

Le cadre légal actuel (LI&L) impose au responsable de traitement : **des formalités préalables** auprès de la CNIL selon la nature des données ou la finalité du traitement ; **une obligation de sécurité** – des mesures logiques, physiques et organisationnelles afin d'assurer la sécurité des données (art. 34 LI&L). Le manquement à cette obligation est puni de 5 ans de prison et 300 000 € d'amendes pour une personne physique et 1 500 000 € pour une personne morale. Les fournisseurs de service de communication électronique doivent notifier sans délai à la CNIL la violation de données à caractère personnel[41] ; **une obligation de confidentialité**.

- **Les obligations issues du RGPD : un nouveau paradigme de responsabilité**

[38] Présentation par le cabinet *KGA Avocats*, voir https://kga-avocats.fr/web/
[39] Article 47 LRN
[40] Article. 43 ter LI&L
[41] « *Toute violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement dans le cadre de la fourniture au public de services de communications électroniques.* » – art. 34 bis LI&L.

Le RGPD impose de nouvelles obligations et responsabilités au responsable de traitement et au sous-traitant. À ce titre, **la responsabilité du sous-traitant pourra être engagée directement**. Le RGPD consacre également **la notion de responsabilité conjointe** des responsables de traitement. Le RGPD instaure le DPO (*Data Protection Officer*), renforce les obligations de sécurité, les pouvoirs des CNIL et les sanctions. Il concerne les «données à caractère personnel»[42]. Le RGPD étend le champ d'application territorial de la protection des données à caractère personnel. Le RGPD s'applique au responsable de traitement et au sous-traitant situé sur le territoire de l'Union européenne mais également au responsable de traitement établi hors de l'Union européenne qui propose des biens et des services à des personnes résidant au sein de l'Union européenne ou qui observe le comportement de ses personnes pour analyser leurs préférences.

La loi européenne impose une nouvelle forme de responsabilité **vers plus « *d'accountability* ». Là se situe le changement de paradigme**. **Le traitant et le sous-traitant de l'information devront pouvoir faire la preuve qu'ils ont documenté leur gouvernance des données personnelles**, selon un certain formalisme. **Qu'ils ont mis en place des outils et des procédures de « *privacy by design* » pour protéger dès la conception qu'ils ont tout tenté pour protéger la vie privée et qu'ils ont eu recours pour ce faire à des notes d'impact préalables**. Le responsable de traitement devra en effet apporter la preuve qu'il a respecté les dispositions du règlement, que des mesures internes appropriées ont été appliquées et respectées, que la relation avec le sous-traitant a été documentée et qu'il a respecté l'obligation d'audit. Les formalités sont allégées dans le sens où la CNIL n'a plus à être notifiée (mais un registre interne doit être renseigné).

Le RGPD instaure de nouvelles obligations qui traduisent un changement de paradigme. Les formalités préalables sont quasiment supprimées (les responsables de traitement ont néanmoins l'obligation de tenir un registre interne des traitements mis en œuvre) pour laisser place à un système d'autocontrôle des entreprises.

- **Les notions d'*accountability* et de *privacy by design***

Le **RGPD introduit en effet en droit français les concepts d'« *accountability* » et de « *privacy by design* »**. La notion d'« ***accountability*** » **désigne l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données**. La notion de « ***privacy by design*** » **implique que les enjeux liés à la protection des données soient envisagés dès l'origine de tout projet comprenant un traitement de données à caractère personnel** puis, ensuite, **tout au long des différentes étapes de conduite de ce projet**. Le responsable de traitement doit intégrer dès la conception et par défaut la question de la protection des données concernant la définition des moyens d'un traitement et du traitement lui-même dans le but de limiter : la nature des données collectées ; la durée des conservations ; les conditions d'accès.

Remarque : **les solutions techniques** pour protéger les données personnelles **sont relatives et rares**, les produits mis sur le marché devant être certifiés (Critères communs…). La notion de *privacy by design* s'entend dès lors ainsi : « **les personnes doivent être informées de leurs droits et des recours à leur disposition pour les faire respecter** ». Il incombe au responsable de traitement qui désire mettre en place un nouveau traitement d'effectuer une autoévaluation des risques que présente son projet sur la vie privée des individus.

Cependant, cette analyse d'impact n'est requise que dans certains cas et, principalement, lorsque le projet présente des risques importants pour les droits des individus si le responsable du traitement ne prend pas de

[42] « Toute information se rapportant à une personne physique identifiée ou identifiable. Au sens du RGPD, est réputée être une «personne physique identifiable», une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. »

mesures pour les atténuer. Le RGPD envisage notamment les traitements impliquant un profilage des individus, le traitement massif de données sensibles ou de données relatives à des infractions ou mesures de sureté, ou la surveillance systématique à grande échelle d'une zone accessible au public.

- **Nomination d'un DPO (*Data Protection Officer*)**

Le RGPD exige la nomination d'un DPO (*Data Protection Officer*) pour certaines entités – les autorités ou les organismes publics, les organismes traitant des données sensibles ou des données relatives aux condamnations pénales et, enfin, les organismes dont l'activité de base implique un suivi régulier systématique et à grand échelle de personnes concernées. La désignation d'un DPO est fortement recommandée par le G29 (qui regroupe les CNIL européennes) même quand sa désignation n'est pas obligatoire.

Le **DPO doit être le point de contact avec le conseil d'administration** et **sera directement rattaché aux instances de direction**. Il doit bénéficier du soutien de l'organisme qui le désigne (implication dans toutes les questions relatives à la protection des données, accès facilité aux données et aux opérations de traitement, indépendance, etc.). Ne pouvant être démis de ses fonctions ou pénalisé à raison de l'exercice de ses missions. Le DPO ne devra avoir aucun conflit d'intérêts avec les missions qu'il exercera[43]. Ses missions sont d'informer et conseiller le responsable du traitement, le sous-traitant et les employés, contrôler a priori les traitements à risque, superviser les audits, donner son avis sur les études d'impact. Les personnes concernées peuvent directement le saisir mais le RGPD ne lui prévoit pas un droit d'alerte. Il est le point de contact avec la CNIL.

- **Le renforcement des obligations de sécurité**

Si le règlement généralise la notification des failles, la question de la suspicion ou le constat de « *breach* » sans que l'intégrité des données ait été constatée laisse une porte ouverte à une interprétation. Le DPO doit-il faire remonter tous les incidents ? Quelle pourrait être la jurisprudence ?

Réponse : **en matière pénale (LI&L), l'interprétation du texte est stricte**. Le juge ne peut donc pas sanctionner des actes que le législateur n'a pas expressément décidé de réprimer. Néanmoins, la réactivité et la coopération dont aurait fait preuve le DPO envers la CNIL pourrait être prise en considération dans l'hypothèse d'une éventuelle sanction du responsable de traitement.

Le terme de *security event* est souvent usité. Selon la norme ISO, un incident est caractérisé dès lors qu'il entraîne une violation de données, un *data breach*. Comment caractériser un *security event* dans le cas d'un Opérateur d'Importance Vitale ? **Voir annexe 1 « La notion d'incident de sécurité à travers les normes et les textes réglementaires »**.

[43] Independant European Advisory body on data protection, Working Party, *« Guidelines on Data Protection Officers (DPO)»,* adopted on 13 December 2016.
À cet égard, le G29 recommande que le DPO n'exerce pas en parallèle un poste pour lequel il serait amené à déterminer les finalités et moyens d'un traitement de données à caractère personnel. Il ne peut cumuler ses fonctions avec celles de directeur des systèmes d'information (DSI) et de directeur du Marketing ou des RH. Il doit faire preuve d'une expertise dans le domaine de la protection des données à caractère personnel. Il est enfin soumis au secret professionnel. Son statut est proche de celui de l'auditeur au sens anglo-saxon du terme.

VIII.1.b. Quelle responsabilité pour les dirigeants d'entreprise

Le **changement de paradigme** se manifeste dans les nouvelles obligations mises à la charge du responsable de traitement et du sous-traitant par le RGPD (qui implique la mise en place d'une gouvernance du risque cyber en interne) mais également dans **les risques accrus de mise en cause de la responsabilité des dirigeants d'entreprise du fait de ces nouvelles obligations**.

À titre liminaire, il convient de relever qu'en cas de faille de sécurité, le responsable de traitement et le sous-traitant **peuvent être à la fois victime et responsable**. Le cas *Orange* en est une illustration. En 2014, *Orange* a été victime d'un vol de données de ses clients hébergées par un sous-traitant. Pour autant, la CNIL a sanctionné *Orange* par avertissement public considérant qu'*Orange* était responsable pour ne pas avoir mené un audit de sécurité de la solution proposée par son sous-traitant.

- **Responsabilité du responsable de traitement et du sous-traitant**

Les obligations en matière de protection des données personnelles pèsent sur le responsable de traitement et sur le sous-traitant, qui sont pour une large part des personnes morales. De même, **l'action de groupe en matière de données personnelles**, lorsque les conditions de sa mise en œuvre seront réunies, **sera dirigée contre le responsable de traitement ou le sous-traitant, c'est-à-dire contre la personne morale**.

Pour autant, les obligations mises à la charge de l'entreprise en matière de données personnelles, avec des sanctions de plus en plus lourdes, sont une source potentielle de responsabilité pour les dirigeants.

- **Responsabilité des dirigeants**

D'une manière générale, en matière de sociétés commerciales, les dirigeants visés sont : pour les SA – le PDG, le président du conseil d'administration, le directeur général, le directeur général délégué, les administrateurs, les membres du directoire ; pour les SAS – le président, le directeur général, le directeur général délégué ; pour les SARL – le gérant.

La responsabilité des dirigeants peut être engagée **sur le terrain civil** (objectif : obtenir réparation du préjudice causé) ou **sur le terrain pénal** (objectif : répressif en cas de commission d'une infraction).

- **Responsabilité civile**

En cas de faille de sécurité et de mise en cause consécutive de la responsabilité civile de la personne morale, celle-ci pourrait se retourner **contre son ou ses dirigeants par le biais de l'action récursoire** afin d'obtenir réparation de son préjudice si la démonstration peut être faite qu'une faute a été commise par le dirigeant qui a conduit ou a participé à la mise en cause de la responsabilité de la personne morale.

La responsabilité du ou des dirigeants pourrait également être engagée, **dans le cadre de l'action sociale**, **par le représentant légal** (rare en pratique, sauf si la société a plusieurs dirigeants), **par un actionnaire** ou un **groupe d'actionnaires** afin d'obtenir réparation du préjudice subi par la personne morale, ou dans le cadre de l'action individuelle, par un actionnaire ayant subi un préjudice distinct de celui de la personne morale.

La responsabilité civile du ou des dirigeants peut être engagée **en cas d'infraction aux dispositions légales et réglementaires**, de violation des statuts et/ou de faute commise dans le cadre de sa gestion (qui peut être une faute intentionnelle ou une faute de négligence ou d'imprudence). **En matière de risque cyber, c'est principalement sur le terrain de la faute de gestion, et plus spécialement de la faute d'imprudence ou de négligence, que la responsabilité du ou des dirigeants pourrait être recherchée**.

Un tiers ne peut engager la responsabilité d'un dirigeant que si celui-ci a commis une faute séparable de ses fonctions (définie par les tribunaux comme une faute intentionnelle d'une particulière gravité incompatible avec l'exercice des fonctions).

En dehors de ces cas, la mise en cause de la responsabilité de la personne morale **peut également conduire à la démission « forcée » du dirigeant**, comme dans le cas de l'entreprise américaine *Target*[44] ou à sa révocation.

- **Responsabilité pénale**

Le risque de mise en cause de la responsabilité pénale des dirigeants en matière de données personnelles **est limité dès lors que les infractions et sanctions énumérées aux articles 226-16 à 226-24 du code pénal visent la personne responsable du traitement de données qui est la personne morale** dans la grande majorité des cas. Néanmoins, dans des cas particuliers, les tribunaux ont parfois été amenés à condamner pénalement des dirigeants.

- **Responsabilité du DPO**

En cas de non-conformité avec le RGPD, la responsabilité personnelle du DPO ne peut être recherchée (au risque que cette nouvelle fonction ne trouve pas de volontaire pour l'exercer). **Néanmoins, certaines questions restent en suspens** : le DPO peut-il être licencié pour faute en cas de mise en cause de la responsabilité du responsable de traitement ou du sous-traitant ; quel est le rôle et la responsabilité du DPO du sous-traitant face à celle du DPO du responsable de traitement.

- **Dans le cadre d'un GIE**

Compte tenu du régime de solidarité existant entre les membres du GIE, les responsabilités encourues seront-elles les mêmes pour les dirigeants ayant un véritable pouvoir de direction (DG, DGD, membres du directoire) et pour les autres dirigeants (administrateurs) ? Seront-elles individuelles ou collectives ? **La responsabilité des membres du conseil d'administration pourrait être engagée sur le terrain de la faute de gestion**, la faute la plus communément reprochée aux administrateurs étant le défaut de surveillance de la direction (faute de négligence). **D'où l'importance pour les conseils d'administration d'inscrire le risque cyber à l'agenda de leurs réunions, de faire remonter les informations par les comités d'audit, d'interroger la direction sur les mesures mises en place**. Le RGPD apporte peu de précision sur l'organisation des relations entre le DPO et le conseil d'administration. Il précise seulement que le DPO fait directement rapport au « plus haut niveau de la direction ».

On peut également s'interroger sur la question de la responsabilité des dirigeants dans le secteur public.

VIII.1.c. Comment limiter la responsabilité des dirigeants face aux dispositions du RGPD ?

- **Instaurer une gouvernance du risque cyber**

En cas de faille de sécurité, les sanctions infligées par les autorités de contrôle seront fonction de la capacité de l'entreprise et de sa direction à **démontrer** que des mesures avaient été mises en œuvre pour éviter les cyberattaques ou pour en limiter les conséquences.

Les entreprises doivent donc **mettre en place des bonnes pratiques permettant de démontrer qu'une interaction entre les équipes dédiées à la gestion du risque cyber existe**.

[44] Démission du PDG suite à une attaque cyber ayant conduit au vol de millions de données bancaires des clients.

Les conditions seront appréciées sur les critères suivant : **la gouvernance doit être est organisée et effective** ; **un plan de formation** existe en interne à destination des DSI, RH etc. à des fins de sensibilisation et de mise à jour des procédures par l'identification de scénarios et l'élaboration de protocoles d'action ; **des outils dédiés ont été créés** (guidelines, chartes d'usage, procédures d'études d'impact par type de traitement avec implication des personnes et des méthodologies) ; que les certifications CNIL et qu'**un code de bonne conduite** reprenant les dispositions du RGPD ont été mis en place ; les bonnes pratiques pour répondre à une attaque cyber sont connues : comment s'effectue le dépôt de plainte, avoir connaissance des niveaux de qualification des infractions, de l'évaluation du niveau de gravité, des procédures de notification à la CNIL et à l'ANSSI et aux personnes concernées.

Attention toutefois, la certification ne diminue pas la responsabilité du responsable de traitement ou du sous-traitant.

- **Le délai de notification de 72h en question**

Quid du délai court (72h) pour notifier une faille de sécurité à la CNIL compte tenu du temps nécessaire pour que le COMEX soit informé et se saisisse du problème ?

Réponse et recommandation : l'une des bonnes pratiques à mettre en place **est la constitution d'une équipe dédiée** de type cellule de crise capable de réagir rapidement en cas de faille de sécurité.

- **Aménager les responsabilités en interne par le biais des délégations de pouvoir**

La délégation doit, **pour avoir un effet exonératoire**, répondre à **certaines conditions** : elle doit être **expresse**, **limitée et précise dans son objet** ; le déléguant doit détenir l'autorité au sein de son entreprise (en pratique il ne peut s'agir que du chef d'entreprise) ; la délégation doit se justifier par l'impossibilité pour le déléguant d'assumer seul le respect de la réglementation ; le délégataire doit être un préposé du chef d'entreprise pourvu de la compétence, de l'autorité et des moyens nécessaires pour assurer l'efficacité de la délégation. En pratique, l'efficacité des délégations de pouvoir en interne **est appréciée en fonction de l'autorité du délégataire et de son degré de subordination**. **En cas de faute commise, nombre de délégations sont requalifiées a posteriori**.

- **Aménager les responsabilités avec les prestataires**

La délégation doit, **pour avoir un effet exonératoire**, répondre à **certaines conditions** : elle doit être **expresse**, **limitée et précise dans son objet** ; le déléguant doit détenir l'autorité au sein de son entreprise (en pratique il ne peut s'agir que du chef d'entreprise) ; la délégation doit se justifier par l'impossibilité pour le déléguant d'assumer seul le respect de la réglementation ; le délégataire doit être un préposé du chef d'entreprise pourvu de la compétence, de l'autorité et des moyens nécessaires pour assurer l'efficacité de la délégation. En pratique, l'efficacité des délégations de pouvoir en interne **est appréciée en fonction de l'autorité du délégataire et de son degré de subordination**. **En cas de faute commise, nombre de délégations sont requalifiées a posteriori**.

On peut s'interroger sur la possibilité pour le dirigeant de déléguer une partie de ses pouvoirs au DPO compte tenu du statut particulier de ce salarié (indépendance notamment) ?

VIII.2. La responsabilité des dirigeants face au risque cyber, le transfert vers l'assurance, *AIG*[45]

Les conséquences de la responsabilité des dirigeants peuvent être transférées à l'assurance suite à un incident cyber du fait d'une action en justice ou d'une action intentée par des investisseurs mécontents des conséquences subies par l'entreprise. De nombreuses victimes peuvent, en effet, mettre en cause les dirigeants (actionnaires, salariés, créanciers, autorités régulatrices, clients...).

Les TPE et les PME ne se sont pas encore saisis de la problématique des données personnelles et du RGPD. Leurs préoccupations en termes de risque cyber portent actuellement davantage sur les menaces liées aux *ransomwares* et sur la protection de leur secret professionnel. Le lien entre la panne de site, la panne informatique et l'attaque cyber n'est souvent pas établi de façon automatique. Il faut encore de longs mois pour découvrir qu'une attaque cyber a eu lieu. Le délai de 72h de notification de toute faille de sécurité à la CNIL imposé par le RGPD parait donc à ce jour hors du scope des pratiques des TPE et PME.

VIII.2.a. Les points essentiels de la couverture

- **Les assurés**

Les polices D&O (*Directors and Officers*), dites responsabilité des dirigeants (RDD) ou RCMS couvrent trois qualités d'assurés qui sont des personnes physiques :

  - **Les dirigeants de droit** qui comprennent également des présidents d'association Loi 1901.
  - **Les dirigeants de fait** (définis par la jurisprudence comme étant toute personne accomplissant en toute souveraineté et indépendance des actes positifs de gestion et de direction engageant la société) sont aussi couverts dans ces polices d'assurance et voient leurs frais de défense généralement pris en charge par les assureurs avant que le tribunal ne statue définitivement sur cette qualité en fin d'instance.
  - **Les dirigeants additionnels** : les assureurs assez communément ont ainsi décidé, en amont, d'octroyer la qualité de dirigeant à toute personne exerçant des fonctions de contrôle, de supervision et de management au sens large. **Le débat concernant la délégation de pouvoir est clos car précisé ainsi par l'assurance** : « que ces personnes aient ou non une délégation de pouvoir, que ces personnes aient ou non un mandat ». Ces dernières années, de nouveaux éléments ont été rajoutés – les dirigeants additionnels tels que les *Data Privacy Officer*, le correspondant CNIL, le président du comité d'audit et du comité de rémunération, les directeurs de la stratégie, du juridique et des assurances. Cette définition des assurés est d'autant plus large que la liste de ces assurés additionnels est en principe indicative comme l'atteste l'adverbe « notamment ».

En matière de périmètre, la police ne précise pas une liste des fonctions. Les dirigeants passés, présents et futurs de la maison mère ainsi que ceux de ses filiales sont couverts par le contrat et ce dans le monde entier. Lorsque les dirigeants assurés poursuivis sont décédés, l'assurance bénéficie néanmoins aux héritiers, aux légataires, ayants cause ainsi qu'aux conjoints, concubins et pacsés du fait de la communauté de patrimoine. **L'employé est également assuré** lorsqu'il est mis en cause conjointement avec un dirigeant de droit ou de fait.

Cette assurance vise ces personnes physiques pour leur éviter d'engager leur patrimoine personnel afin de payer les dommages et intérêts ainsi que pour pourvoir à leur défense. En effet, tout dirigeant qui puiserait dans les fonds de la société pour payer un avocat ou qui requerrait aux services d'une direction juridique pour

[45] Présentation par *AIG*. Voir https ://www.aigassurance.fr/

sa défense personnelle serait en situation d'abus de bien social. Les administrateurs et les responsables nomment une personne physique qui vote au Conseil d'administration. Cette personne possède également la qualité d'assuré.

- **Le contrat**

Il est souscrit par la société pour le compte de ses dirigeants. Afin d'avoir le périmètre couvrant le plus d'entités possible, **il est conseillé que le souscripteur soit l'entité la plus haute de l'organigramme**. Le contrat doit être adapté aux juridictions françaises et étrangères. Les contrats ont généralement une territorialité monde entier – dès lors que les dirigeants des filiales sont couverts dans le monde entier (toutes nationalités), ils peuvent être mis en cause par des tiers de toutes nationalités, devant toutes les juridictions au niveau du monde.

- **La faute**

Elle peut être liée au :

  - **manquement aux obligations légales ou réglementaires** entendues au sens large – l'assurance ne comporte pas encore de restriction ni rien de spécifique aujourd'hui aux enjeux cyber dans les polices D&O.
  - **la violation des statuts** : notamment l'objet social des PME (souvent le document a été rédigé bien avant l'existence des nouvelles technologies). Il est utile et important de remettre à jour les statuts et l'objet social de la société avec un avocat pour ne pas être en situation de violation de statuts, une situation très facile à activer pour un tiers.
  - **la faute de gestion** : toute faute commise par négligence, imprudence, omission, erreur ou déclaration inexacte – la définition par l'assurance ne pouvant pas être plus large.

VIII.2.b. Les acteurs de la mise en cause des dirigeants

- **La société**

La société elle-même peut mettre en cause ses propres dirigeants à l'occasion d'une crise de gouvernance etc. Le nouveau conseil d'administration au titre de la société peut mettre en cause l'ancienne équipe dirigeante à la fois pour défendre les intérêts de la société et pour marquer son entrée en fonction, une situation courante.

- **Les fournisseurs**

Les **fournisseurs**, les **créanciers**, le **liquidateur amiable ou l'administrateur judiciaire** suite à une mise en cessation de paiement de l'entreprise et/ou à sa faillite cf. la loi du 25 janvier 1985, revue par la loi du 26 juillet 2005 et plus récemment amendée par la loi Sapin 2 du 9 décembre 2016 – sur l'action en responsabilité pour insuffisance d'actif, qui en substance disposent qu'un juge de tribunal de commerce peut, dès lors qu'une cessation de paiement ou des dettes sont constatées suite à une faute de gestion, faire supporter cette dette à tout ou partie des dirigeants (droit ou de fait) et de manière individuelle ou solidaire. La faute de gestion est définie par la jurisprudence. On peut supposer que si une société dépose le bilan suite à un incident cyber dont elle ne se remet pas, les personnes ayant des dettes pourraient mettre en cause via le tribunal les dirigeants à titre de personnes physiques puisque l'argent est là, et derrière les dirigeants, il y a des contrats d'assurance qui créent cette solvabilité. Ce cas de figure arrive souvent même si des progrès ont été faits pour éviter les faillites d'entreprise. Aujourd'hui, la seule limite à de telles actions est l'engorgement des tribunaux – ex. le tribunal de Bobigny ne traite que les passifs supérieurs à 5M€, 500 000€ en Corrèze. Ces situations sont très fréquentes pour les PME – le vrai risque pour un dirigeant est la faillite et qu'on lui attribue la

responsabilité du remboursement des dettes. Même cas de figure pour la SARL, car la responsabilité est certes limitée pour l'associé mais pas pour le gérant. Situation très fréquente pour les PME.

- **Les actionnaires ou les associés (pour le compte de la société ou pour leur propre compte)**

Les actionnaires ou **les associés** peuvent mettre en cause les dirigeants si le cours de l'action dévisse (cas *Target*). Aux États-Unis, les avocats des actionnaires peuvent déposer en moins de deux heures des plaintes et envoyer des *class actions* avec des demandes peu motivées en termes d'allégation des faits et cela pour un montant astronomique.

- **Les autorités administratives**

Les autorités administratives peuvent mener des enquêtes contre la personne morale et contre les personnes physiques. Elles exercent un pouvoir de sanction tant en France qu'à l'étranger – les filiales à l'étranger sont concernées.

VIII.2.c. Les acteurs de la mise en cause des dirigeants lors d'un incident cyber

Tous ces acteurs peuvent intenter un recours judiciaire. Les **associations de consommateurs** pourront jouer un rôle demain dans leur aptitude à mener des actions de groupe[46]. Toutes n'ont pas la capacité financière d'intenter une telle action en justice en France. À la différence d'il y a deux ans, où cinq ou six actions ont été engagées en six mois, il se pourrait qu'à l'avenir leur stratégie soit d'engager une action majeure.

- **L'objet de la police**

Il s'agit de **garantir la responsabilité personnelle de l'ensemble des dirigeants de l'entreprise dans le cadre de manquements aux obligations légales et/ou réglementaires, de violation des statuts ainsi que de fautes de gestion, en protégeant le patrimoine personnel de leurs dirigeants.**

L'assureur prend en charge **les frais de comparution**, **les frais de défense** (à ne pas confondre avec la notion de protection juridique car il s'agit ici de défense face à une mise ne cause et non d'un recours contre un responsable) et **les éventuels dommages et intérêts auxquels ils pourraient être condamnés** si reconnus responsable des dommages causés. **Les dirigeants ont généralement le libre choix de leur avocat mais en contrepartie ont aussi l'obligation de se défendre, de contester la réclamation qui leur est faite** – à l'exception des enjeux liés aux procédures de plaider coupable dans les pays de *common law* pour lesquelles l'assureur doit être associé à la conduite de la stratégie de défense. **L'indemnisation d'assurance n'est pas assortie d'une franchise lorsque l'assuré pris en charge est une personne physique** – sauf pour les pays de *common law* dans lesquels la société a le droit statutaire de prendre en charge les indemnités mises à la charge des dirigeants poursuivis en leur lieu et place. **Dans le cas où la société peut indemniser, les assureurs avancent ou remboursent à la société cette somme déduction faite d'une franchise**. Aucun barème n'est imposé ni le choix d'avocat (sauf panel suggéré parfois et susceptible d'aménagements). Le seul encadrement de ces polices – les frais doivent être nécessaires et raisonnables.

Les points essentiels de la couverture lors d'un incident cyber

- **Le Sinistre Maximum Possible (SMP) : PME vs grands groupes**

[46] Le règlement (UE) 2016/676 (art. 80) instaure le principe de la class action.

Le « SMP » de la PME suite à une attaque cyber est **la faillite** pouvant entrainer une action en cas d'insuffisance d'actifs à l'encontre du dirigeant si celui-ci a commis une faute soit dans la gestion de cet incident cyber soit dans les moyens de prévention. Ces actions ont un coût élevé pour l'assurance.

Le « SMP » **pour un grand groupe coté suite à une attaque cyber se traduit davantage par une réclamation d'actionnaires du fait d'une possible perte de valorisation de leurs titres financiers à l'encontre de la personne morale émettrice**. Un **décroché de cours de bourse de plus de 20%** par rapport à l'indice sur une période de vingt-quatre à quarante-huit heures est très souvent suivi aux États-Unis par une *class action*. Les demandes s'expriment en milliards comme base de discussion, avant d'aboutir à une transaction. Les *plaintiff lawyers* prenant un pourcentage. **Dans ces cas-là sont mis en cause : l'équipe dirigeante et conjointement, ou seule, la personne morale**. **Les contrats étendent la qualité d'assuré, non plus aux personnes physiques mais aussi à la personne morale dans les seuls cas de réclamations relatives aux sinistres boursiers** (dans ce cas également une franchise pourra s'appliquer puisque l'assuré couvert est une entité morale). **L'assurance ne couvre pas les enquêtes et les investigations préalables** menées par les autorités régulatrices, en dehors de tout contexte de faute alléguée, contre la personne morale parce qu'elles se chiffrent en dizaines de millions de dollars et parce qu'il relève du risque d'entreprise de se conformer aux réglementations en vigueur.

Pour ces gros sinistres, les achats de garantie pour les grands groupes se situent entre cent millions et quatre cent millions de dollars par période d'assurance. Pour de tels litiges boursiers en 2001, la majorité des couvertures ont parfois été épuisées uniquement par des frais de défense. Les *plaintiff lawyers* facturent entre un et deux millions de dollars par mois par dossier.

- **Amendes civiles et administratives suite à un incident cyber : débat sur leur assurabilité (voir en annexe 4 - la note FFA Assurabilité des Amendes administratives)**

Les montants financiers visés par le RGPD sont importants mais ils sont du même ordre que pour le blanchiment ou la corruption. Le problème n'est donc pas le montant du point de vue de l'assurance.

En revanche, la non-assurabilité des amendes civiles et administratives a pour conséquence que très peu de personnes acceptent désormais d'assumer de tels risques dans le cadre de leurs fonctions. Une solution doit être trouvée par le marché qui apporte aujourd'hui des réponses variées.

Une importante littérature existe sur cette question de l'assurabilité des amendes civiles entendue au sens large – à celles de CNIL, de l'AMF etc. Les zones grises du débat concernent le maintien ou non du caractère coercitif de l'amende si celle-ci est prise en charge par l'assurance. En fonction du montant de l'amende, le caractère intentionnel ou non des faits qui ont conduits à l'amende peut être évalué et donc son assurabilité. Une amende d'un million d'euros traduit un niveau de gravité important et un caractère intentionnel des faits qui la rend inassurable. A l'inverse de petites amendes traduisant une imprudence ou une négligence qui peuvent être prises en charge par l'assurance.

Les dispositions impératives de la Loi française ne sont pas clairement définies. Les sociétés d'assurance souhaitent une clarification du sujet par les autorités afin que l'ensemble des entreprises, exerçant sur le marché français, puissent partager des positions communes sur cette question en dehors de tout contexte de compétitivité contractuelle. En effet, la position de la non assurabilité des amendes n'est pas partagée par tous les acteurs. Certains assureurs ont pris des positions différentes, notamment concernant la prise en charge des amendes dites civiles et plus précisément des sanctions financières prononcées par des autorités administratives indépendantes (telles que la CNIL ou l'AMF). Force est de garder à l'esprit la nécessaire sécurité juridique qui est due aux assurés au travers des engagements pris par les assureurs. Contrairement à un sinistre de dommage, de perte d'exploitation ou de RC classique, un sinistre mettant en cause la

responsabilité des dirigeants s'apparente souvent à une gestion de crise de par l'importance des personnalités poursuivies.

Le débat avec le régulateur doit être clarifié pour savoir si *in fine* l'objectif est de fournir une solvabilité pour les autorités de tutelle voire même pour le régulateur ou si au contraire, le but est l'exemplarité de la sanction qui peut être dure lorsqu'on n'est pas dans une faute purement intentionnelle. Le *risk manager* et le courtier doivent être amenés à se poser les bonnes questions préalablement au prononcé de toute sanction et aux légitimes doutes que l'on peut avoir sur la légalité de leur prise en charge par l'assureur eu égard au principe de personnalité des peines et à la nullité de clauses de contrats contraire à la préservation d'un ordre public économique. Une distinction doit être faite entre d'un côté des dommages et intérêts (même punitifs) qui ont pour vocation d'indemniser des tiers victimes de fautes de gestion commises par un dirigeant et de l'autre côté des sanctions qui sont libellées par un régulateur et perçues par le Trésor public dans un but de sanctionner un comportement qui a porté atteinte à l'ordre public économique dont ils sont garants.

Le débat sur cette prise en charge n'est pas propre à l'assureur mais concerne également la société elle-même afin de savoir jusqu'où elle peut contribuer directement ou non à apporter une protection financière à son dirigeant sanctionné. Ne serait-ce que le fait d'autoriser un programme d'assurance, qui a été payé par la société, à couvrir une sanction inassurable peut être constitutif d'une faute de gestion contraire à l'intérêt social.

Il convient de souligner qu'en France, ce type de contrat demeure la seule protection financière aujourd'hui pour des dirigeants en droit français et que son champ d'application se doit de respecter les règles impératives conforme à l'ordre public[47].

Voir également **en annexe 3 – une analyse juridique complémentaire de l'assurabilité des sanctions pécuniaires**.

VIII.2.d. Responsabilité des dirigeants dans les grandes entreprises : la communication financière

Sur la base des rapports annuels de l'année 2015 publiés en 2016, 68% des sociétés du SBF120 communiquent sur les *data* et sur le risque lié à la protection des données à un moment où un autre. C'était 28% en 2013. **On constate une sensibilité accrue dans le besoin des sociétés de communiquer sur le sujet**. Avec une spécificité française, tous les documents ou prospectifs d'introduction en bourse comprennent un chapitre facteurs de risque. Une soixantaine de pages en moyenne aujourd'hui, contre vingt il y a vingt ans, faisant la liste de tous les risques que prennent les actionnaires à entrer en bourse.

Depuis certains incidents où la responsabilité des dirigeants avait été engagée suite à une mauvaise rédaction du programme assurance, et notamment des franchises dans le rapport annuel, **la France est le seul pays au monde qui dispose d'un chapitre risque et d'un chapitre assurance dans lesquels la société dévoile précisément la manière dont elle est assurée**.

Nous pouvons néanmoins constater que **ces deux chapitres sont rédigés de façon très différentes** : les terminologies ne sont pas les mêmes, les fonctions risques décrivent les risques dont ils ont la charge et les fonctions assurances décrivent les assurances dont ils ont la charge uniquement – et ne pas mentionner l'assurance des personnes, du crédit. Ces deux chapitres ne se correspondent pas. Des risques peuvent être mentionnés sans que soit expliqué comment ces derniers sont assurés ou sans mentionner qu'ils ne le sont

[47] Emmanuel Silvestre, « Les sanctions pécuniaires prononcées par les autorités administratives », Lamy des Assurances – 2017.

pas. Le décalage est important. **Or, dès lors que l'organisation va avoir un problème de *data*, les actionnaires ne vont pas interroger pour savoir si l'entreprise était bien protégée sur le plan technique. Ils vont se référer à ce qui est écrit dans le rapport annuel**. Ils pourraient ainsi faire référence à la façon dont le chapitre risque est rédigé. **Ils liront que le risque n'est pas noté comme important**. Ils se réfèreront au chapitre assurance qui ne mentionne pas d'assurance correspondante. Ils pourraient conclure qu'il y a eu « *misrepresentation* » ou qu'il y a eu mensonge. Et s'ils avaient su ils n'auraient pas acquis des actions. Raisonnement simple.

Aux **États-Unis, la SEC propose aux entreprises privées, depuis le mois de février 2018, un cadre formel pour informer les investisseurs du niveau de maturité cyber de l'organisation** et de remontée d'information concernant les attaques cyber dont elle a été victime[48].

Recommandation

D'ici deux ans très probablement, 100% des sociétés cotées en bourse auront un chapitre risque sur les *data* et 100% auront un chapitre assurance. **La préconisation est de se mettre en situation de risque afin que le jour où le conseil d'administration serait mis en cause la ligne de défense soit prête**, notamment en ce qui concerne la communication financière au sujet des *data*. D'ici deux ans très probablement, 100% des sociétés cotées en bourse auront un chapitre risque sur les *data* et 100% auront un chapitre assurance.

VIII.2.e. Les challenges pour l'industrie de l'assurance

- **Un risque systémique**

Les réassureurs estiment que le principal risque cyber peut être le risque systémique, c'est-à-dire en mesure de déstabiliser l'ensemble de l'industrie de l'assurance.

Pour les assureurs, un risque cyber estimé entre dix ou vingt millions d'euros est gérable. En revanche, si le risque cyber est un virus à effet massif ou un problème de données qui seraient véhiculés par un des GAFA ou un des Big5 … et s'il venait à se disperser sur des milliers d'entreprises, se poserait alors un problème d'accumulation et d'agrégation.

Le risque systémique se décline en trois dimensions : premier cas – **la partie de bowling**, une attaque unique touche plusieurs parties par les flux de données ; second cas – **la partie puzzle** pour savoir quelle couverture chapeaute quelle autre notamment avec la problématique des couvertures silencieuses. Ce problème de cumul est un défi pour les assureurs de RC qui, s'ils décident d'introduire des exclusions, verront, automatiquement et impérativement de par la loi de sécurité financière, les couvertures ainsi supprimées générer des garanties subséquentes dédiées et reconstituées s'enclencher pour une période minimale de cinq années. Lorsque les assureurs RC commenceront à mettre des sous limites sur les polices RC, c'est qu'ils ne seront pas loin de sortir le cyber du champ des couvertures jusqu'à présent accordées sous « *silent form* » (car non exclues) ; troisième cas – **l'effet domino**. Nous ne sommes pas sur des zones de risques qui se cumulent mais qui s'enchaînent les uns aux autres par effet collatéral. On peut imaginer que les salariés ou les membres du conseil d'administration se retournent contre les dirigeants pour n'avoir pas mis en place les mesures de prévention et de protection demandées par les assurances qui auraient pu couvrir cette attaque et ainsi éviter son impact négatif au bilan de la société. Est actuellement observé, concernant la fraude ou le cyber, une certaine libération de la parole dans les entreprises. Même si statistiquement la fraude interne coûte plus cher que la fraude externe, les entreprises parlent plus facilement si l'ennemi est identifié à l'extérieur (cela évite d'aborder une possible et inconfortable suspicion envers ses propres employés).

[48] SEC rel. 33-10459; 34-82746.

- **L'agrégation**

Le second point est qu'une **partie du risque cyber peut être couvert par une police fraude, dommage ou de responsabilité civile**. **Le problème vient également du fait que les impacts cyber sont couverts par les couvertures silencieuses**. Actuellement, le régulateur exerce une pression pour que l'assureur connaisse, estime ou modélise son exposition cyber en tant qu'assureur cyber et également et surtout en tant qu'assureur non cyber pour toutes les couvertures qui sont vendues. Le marché n'est pas encore structuré sur ce point. Une orientation que certains assureurs portent sans que cela soit partagé par tous (n'engageant pas *AIG*) est que, d'ici quelques mois, des exclusions vont apparaître dans les polices dommages ou RC afin de concentrer le cyber dans une police de façon. Selon une démarche proche de celle utilisée pour la modélisation du risque environnemental, il y vingt ans et celui portant sur l'amiante, il y a quinze ans.

VIII.2.f. Retour d'expérience sinistre Cyber : la gouvernance, un élément clé

Neuf fois sur dix dans la réalité des sinistres, les entreprises sont désemparées. Dans les grands groupes, les PCA – plan de continuité d'activité – sont préparés, les cellules de crises existent ainsi que des premiers éléments de gouvernance. Mais le conseil d'administration est en demande d'explication, il met du temps à se réunir et la prise de décision est compliquée. Si la filiale est touchée, la complexité de la situation est démultipliée. Une différence de réactivité existe entre les grands groupes et les PME pour lesquelles la prise de décision est plus simple, pragmatique et compacte à l'inverse des grands groupes dans lesquels intervient une multiplicité d'intervenants intérieurs et extérieurs (ex. sociétés d'IT, des juristes) voir de négociateurs – dans le cas de *ransomwares*- rançongiciel.

Tous les sinistres ne sont pas déclarés. Pourquoi ? Enjeu de réputation ? La majorité des sinistres enregistrés en 2016/17 tourne autour de la cyber-extorsion (fraude au président et/ou rançongiciel).

- **Attaque *Vinci***

Sept milliards de perte d'actif en bourse en sept minutes mais cette attaque n'est pas considérée comme cyber par l'ANSSI[49]. Ce cas illustre pourtant très bien l'impact que peut avoir un incident cyber sur un cours de bourse. Dans les quarante-huit heures suivantes, l'action a repris six milliards. Cet évènement « une rumeur » illustre **l'impact. C'est un cas d'école parfait pour étudier l'impact boursier**. Seuls 40% de ceux qui ont vendu ont ensuite racheté. L'AMF pourrait mettre sept mois pour comprendre ce qui s'est passé. Imaginons. **Si cela devait être un vrai incident cyber, le conseil d'administration aurait été mis en cause aux États-Unis en trois minutes après les sept minutes du décrochage. Il faut « trois minutes » pour que les *class actions* soient envoyées, le *filing* (la procédure d'envoi) est quasi automatique**.

- **Motifs d'achat des polices RCMS vs polices Cyber**

100% des milles sociétés cotées souscrivent une assurance RCMS (Responsabilité Civile des Mandataires Sociaux) depuis quinze ou vingt ans. Mais seules 10% de ces sociétés auraient souscrit une police cyber. Cela s'expliquerait par le fait que les premières polices sont apparues il y a cinq ans sur le marché français mais que cela ne fait que deux ans que le marché commence vraiment à se développer. Désormais, les demandes d'études sont transformées.

Au sein du CAC40, vingt-quatre sociétés sont assurées et huit réfléchissaient en 2016. En 2014, elles étaient sept. L'évolution suit la même progression qu'à l'époque pour la RCMS, les grands groupes entraînent les ETI et les PME.

[49] Voir https://www.ege.fr/download/etude_EGE-Ophois_mars2018.pdf

Si l'on regarde par secteur d'activité, il suffit qu'une grande entreprise inscrive dans son rapport annuel qu'elle est assurée pour que les autres suivent. Ce fut le cas pour la grande distribution et les banques, lesquelles achètent plus encore de polices cyber que les assureurs. Toutes les OIV se sont assurées ou sont en cours. Les opérateurs téléphoniques étant tenus de notifier et le cas d'*Orange* ayant été un cas d'école tous ont acheté. D'autres secteurs d'activités sont peu assurés alors même que leurs données sont sensibles et ciblées tel que le domaine de la santé. De même, il pourrait paraître évident que le e-commerce soit attentif à la perte d'exploitation en cas d'un incident qui bloquerait leur site internet. Les mutuelles, les instituts de prévoyance émettent des demandes mais concrétisent encore peu d'achats.

- **Incident Cyber et responsabilité des dirigeants : le cas *Target***

Target – cent dix millions de victimes fin 2013, environ soixante-dix millions d'identités dérobées dont quarante millions de données bancaires qui ont nécessité pour trois millions d'entre elles une réémission (soit un coût direct de cent soixante millions de dollars), des frais de notification (cent millions de dollars). **Suite à cet incident, le bénéfice net de l'entreprise a baissé de moins trente-quatre pour cent. Le cours de bourse a décroché pour une perte de plus quatre milliards de dollars de valeur boursières**. **Dans les mois qui ont suivi, le PDG et le RSSI ont été remerciés**. **Quatre-vingt poursuites au civil et des *class actions* dont deux contre les dirigeants action**. Les *derivative lawsuits* ont tous été déboutés à l'été 2016 (aucune indemnisation n'a été versée).

La police D&O a été impactée. Soixante-cinq millions de dollars ont été dépensés en frais d'investigation et d'avocats. Tout comme la capacité cyber qui avait été achetée à hauteur de de cent million. Cette attaque faisait suite à d'autres qui avaient eu lieu en 2007. Les membres du *board* étaient au courant de failles de sécurités sur les terminaux de paiement et n'avaient pas pris les mesures nécessaires ce qui a conduit au problème de 2013.

- ***Due Diligence***

Cette société a acquis une assurance cyber en ayant connaissance des failles de 2007. Le *board* était au courant des déficiences, des faiblesses. **Est-ce que la compagnie d'assurance aurait pu faire une *due diligence* ou demander des informations avant de valider l'achat de cette assurance** ? Normalement le processus de souscription implique une réunion entre l'assureur et le RSSI afin d'étudier les mesures de sécurité en place. Le *board* était au courant de cette information comme il peut l'être alors que de très nombreuses attaques ont lieu en grand nombre tous les jours.

Une fois par an, un représentant de l'informatique vient présenter l'état des lieux de la menace sans pouvoir présenter de granularité, de sensibilité d'une gouvernance par rapport à un risque mais des cases sont cochées. Une analogie peut être conduite avec le secteur de la pharmacie où doit nécessairement siéger un pharmacien avec le statut de pharmacien responsable. Une telle évolution est très probable pour le cyber.

IX. La valorisation des biens intangibles et leur gestion d'un point de vue assurantiel

IX.1. Les fondamentaux de la valorisation comptable des données intangibles[50]

IX.1.a. La part de la valeur des biens intangibles dans les entreprises ne cesse de croître

La valeur des entreprises et leur balance sont de plus en plus immatérielles. **Plus de 50 % de la valeur des entreprises aujourd'hui correspond à la valeur des actifs intangibles** que l'on peut lister en quatre grandes catégories : la valeur de **la marque**, de leur **technologie brevetée** ou non, de leur **système d'information** et de leurs **équipes constituées** – terme comptable pour parler du capital humain. Néanmoins **moins de 20% de ces actifs vont être retrouvés au bilan comptable des entreprises**.

- **Biens intangibles et capitalisation boursière**

Pour quelles raisons, ne trouve-t-on pas les actifs intangibles dans les comptes des sociétés ? Les normes comptables internationales, et notamment, l'IFRS et l'AS 38 (l'incorporel), les normes françaises qui se sont alignées interdisent de comptabiliser la plupart des biens intangibles que l'on pourrait trouver dans une société. Dans le cas de ***LVMH***, la valeur de l'incorporel est essentiellement due aux marques – 100 milliards de capitalisation boursière, soit un montant pratiquement équivalent en termes de valorisation de la marque cotée en bourse. Pour ***Sanofi***, la valorisation de la marque correspond à celle du brevet – il est donc principal actif incorporel de cette organisation. La valeur d'***Altran*** est constitutive de ses équipes constituées c'est-à-dire de son capital humain. Le capital immatériel de ***Thales*** s'élève pour sa part à 87%.

Le marché – la bourse – **valorise aujourd'hui principalement l'immatériel selon trois composantes** : le domaine **des marques**, le domaine **des techniques** (brevets) et **du capital humain**.

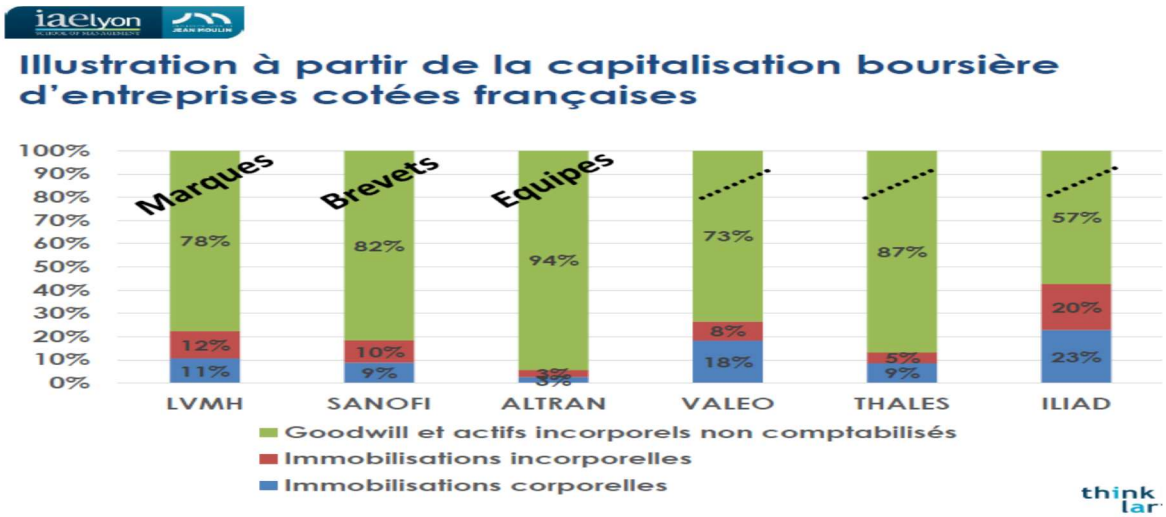


Figure 4 – l'incorporel dans la capitalisation

En vert l'immatériel, en rouge la partie incorporelle comptabilisée – inférieure à 20%. En bleu, la partie immobilisation corporelle qui correspond à des montants extrêmement faibles.

[50] Présentation du Pr Edouard Chastenet de Castaing, Professeur associé, Responsable du Master Ingénierie Financière et Transaction, iaelyon School of Management, Université Jean Moulin, Expert de justice près de la Cour d'Appel de Lyon

Selon la **norme IAS 38**[51], un **actif incorporel** est un actif **non monétaire**, identifiable et sans substance physique. Un actif non monétaire est **identifiable** s'il répond à deux de ces critères au moins : **s'il est réparable** ou **s'il résulte d'un droit légal ou contractuel portant sur un brevet ou une marque**, même si ce droit n'est pas séparable de l'entité ou des autres droits et obligations contractuelles. Cette condition a été rajoutée par les IFRS (*International Financial Reporting Standards*). Un brevet résulte d'un droit légal[52]. Pour être **comptabilisé** en immobilité incorporelle, un actif incorporel doit satisfaire à deux conditions : à la définition d'un actif incorporel et aux critères de comptabilisation d'un actif qu'il soit corporel ou incorporel. **Il s'agit de prouver que les avantages économiques futurs attendus qui sont attribués à l'actif iront à l'entreprise**. Ce qu'il est aisé de faire au titre de la marque.

La deuxième condition doit établir que **le coût de cet actif peut être estimé ou évalué de façon fiable**. Cette seconde condition a ainsi amené **le normalisateur à rejeter la comptabilisation des actifs immatériels générés en interne**. Seul est pris en considération, le coût direct d'un bien intangible lorsqu'il y a acquisition d'un actif incorporel. Dans ce cas, le coût est direct et clair car il correspond au prix de la transaction. En revanche, s'il est créé de façon endogène, l'estimation de sa valeur, que peut en faire l'organisation, ne sera jamais assez fiable (comparable) pour respecter cette condition. Il y a eu un rejet assez direct du normalisateur.

Pour savoir si les actifs sont comptabilisables, **le législateur a réparti les actifs en trois grandes catégories**. Les **actifs incorporels qui ont été acquis séparément** – achat direct d'une marque, acquisition séparée directe ; **acquisition de l'entreprise qui exploite la marque** – achat indirect, acquisition séparée indirecte. Le normalisateur a retenu l'acquisition via un regroupement d'entreprise : la substance l'emportant sur la forme, l'organisation va comptabiliser directement la marque en faisant abstraction du mode d'acquisition de la marque via l'achat des titres. **La troisième possibilité résulte des actifs créés par l'organisation elle-même** (générés en interne). L'entreprise exerce ainsi un contrôle sur l'actif qu'elle a elle-même créé.

iaelyon

Critères de comptabilisation des actifs incorporels (selon la norme IAS 38) - suite

Exemples	Acquis séparément	Acquis via un regroupement d'entreprises	Générés en interne
Marques Relations clients (contrats, fichiers…)	Oui (Prix d'acquisition)	Oui (Juste valeur)	~~Non~~
Technologies (brevets, logiciels…) Systèmes d'informations	Oui (Prix d'acquisition)	Oui (Juste valeur)	Coûts de développement uniquement (recherche : non)
Autres contrats, concessions …	Oui (Prix d'acquisition)	Oui (Juste valeur)	-
Equipes constituées / savoir-faire	~~Non~~	~~Non~~	~~Non~~

think large

Figure 5 – la norme IAS 38

[51] Voir http://www.decformations.com/ftp/ias/ias38.pdf

[52] Mais une technologie non brevetée gardée secrète, n'est pas forcément exploitée par un contrat de licence mais peut contribuer à créer de la valeur dans une entreprise. Cela va par exemple, être le cas d'une formule secrète jamais brevetée (ex. Coca-Cola). On peut considérer que cette formule secrète peut être vendue ou concédée par licence à un tiers selon le principe que la substance l'emporte sur la forme juridique. Même sans protection juridique et sans contrat, en substance, l'organisation peut prouver qu'elle exerce un contrôle sur l'actif incorporel.

En fonction de ces trois possibilités d'acquisition ou de prise de contrôle de l'actif, le normalisateur a déterminé quelles sont les possibilités de comptabilisation.

Si une marque a été acquise séparément ou via un regroupement d'entreprise, dans le premier cas, son prix effectif est déterminé par le **prix d'acquisition**. Dans le cadre d'une acquisition de regroupement d'entreprises, le coût précis de la marque étant inconnu un autre référentiel de valeur va être utilisé : la **juste valeur de cette marque**. Des évaluateurs déterminent la juste valeur de l'entreprise sont des méthodes d'appréciation des valeurs incorporelles. **Si la marque a été créée par l'entreprise cette dernière n'a pas le droit de la comptabiliser** car les méthodes qu'elle aura utilisées pour elle-même en interne ne sont pas suffisamment fiables. Au niveau des comptes consolidés d'une entreprise et de ses filiales, la règle est la même.

En revanche, au niveau des comptes sociaux de la filiale, la situation est différente. Si une marque est localisée dans une filiale en France et qu'elle est cédée à une autre filiale dans un autre pays, un prix de transfert devra être déterminé. **A quel prix met-on à disposition l'actif incorporel entre le siège social et les filiales ? C'est l'administration fiscale et non pas les commissaires aux comptes qui va déterminer le juste prix**.

Pour quelle raison, l'évaluation du juste prix ne peut pas être faite en interne ? Le fait qu'il y ait une valeur globale de l'entreprise qui couvre celle des actifs incorporels donne, en quelque sorte, un cadre dans lequel on a moins de chance de se tromper car on connaît le coût global de la marque ainsi que le coût de l'acquisition, la différence des deux constituant le coût des actifs incorporels. Le prix d'acquisition de l'entreprise est considéré comme juste valeur puisqu'il résulte d'un accord entre le vendeur et l'acheteur – lequel constitue le référentiel qui couvre la valeur des biens incorporels. Cette valeur globale de l'entité constitue un cadre. **L'objectif du normalisateur est de lutter contre l'erreur et le risque de manipulation comptable**.

L'évaluateur intervient dans trois contextes : **le traitement comptable lors de regroupement d'entreprises**, **les prix de transfert au sein de groupes internationaux**, **des opérations transactionnelles** qui ne sont pas des OPA dans la mesure où elles ne mettent pas en rapport des tiers dans une négociation. Exemple, la vente de la marque créée par l'entrepreneur qui vend en même temps son entreprise et la marque lors d'une même opération financière – la marque étant vendue à titre personnel car c'est lui-même qui l'a créée. **L'évaluateur intervient pour déterminer une valeur qui sera aussi une référence pour l'administration fiscale puisque l'entrepreneur sera taxé sur les plus-values au niveau de cette session**. En revanche, dans le cas des fusions acquisitions, l'évaluateur n'intervient jamais car les opérations ne portent pas sur les marques en tant que telles et généralement l'acquéreur et le vendeur négocient sur des critères qui ne sont pas ceux de la marque.

IX.1.b. Comptabilisation des coûts de développement en interne entreprise

Il existe des critères très précis pour pouvoir comptabiliser les coûts de développement. La qualification des actifs incorporels générés en interne en tant que coûts de développement suppose en effet la réunion de six critères :

- La faisabilité technique nécessaire à l'achèvement de l'incorporel ;
- L'intention de l'acheter en vue de son utilisation ou de sa vente – démontrer une confirmation par le top management de l'entreprise ;
- La capacité à l'utiliser ou à le vendre – démontrer la capacité à utiliser l'actif incorporel une fois qu'il est développé soit par l'utilisation interne soit par la vente ;
- La façon dont il a généré des avantages économiques futurs et probables (existence d'un marché ou d'une utilité interne) – démontrer l'existence d'un marché ou l'utilité interne pour quantifier, montrer l'existence d'un business plan avec des flux de trésorerie future ;

- La disponibilité des ressources nécessaires à son achèvement – démontrer que l'on dispose de la capacité en interne ;
- La capacité à évaluer de façon fiable les dépenses qui lui sont attribuables au cours de son développement – complexe : collecter les fiches de temps.

Ces critères étant très restrictifs, de nombreux actifs incorporels technologiques ne sont pas inscrits au bilan parce que la part des coûts de recherche est beaucoup plus importante que le coût de développement.

Une entreprise peut donc aisément ne pas « réussir » à qualifier un actif d'intangible[53].

Le cas principal où une grosse partie du coût de l'actif peut être comptabilisé comme un actif intangible concerne **les systèmes d'information et le développement de certains logiciels** selon 6 critères.

Les contrats et les cessions acquis directement dans le cadre de regroupement d'entreprises sont valorisable selon les règles de comptabilisation d'entreprise.

Tout ce qui relève du capital humain n'est jamais comptabilisé car il n'appartiendra jamais qu'à l'homme. **Tout le savoir-faire associé à ces équipes ne peut pas être comptabilisé**.

Très peu d'actifs incorporels générés en interne sont comptabilisés d'où cet écart très important entre valeur boursière et valeur comptable.

- **La valorisation des biens intangibles dans le cadre d'un regroupement d'entreprises, appréciation de la juste valeur**

iaelyon

S'agissant de la Juste valeur (actifs acquis dans le cadre d'un regroupement d'entreprise)

Exemples	Approche par les coûts	Approche par les revenus	Approche par marché
Marques	Non/Oui : Marques récentes	Oui *	Non
Relations clients (contrats, fichiers…)	Non/Oui : Fichiers	Oui *	Non
Brevets	Non/Oui : Brevets récents	Oui *	Non
Logiciels (droits d'auteur)	Oui	Oui *	Non
Systèmes d'information	Oui *	Non	Non (sauf éléments comparables)
Equipes constituées	Oui *,**	Oui *,**	Non

* Approche principale ; ** évaluées mais non comptabilisées

think large

Figure 6 – Appréciation de la juste valeur

[53] Dans l'industrie pharmaceutique, le développement nécessite de nombreuses années mais on considère que l'entreprise ne fait plus de recherche et rentre dans la phase de développement dès lorsqu'elle obtient les ADMM : l'autorisation de mise sur le marché. « Dix années de recherche » ne peuvent pas être activées, seuls les coûts de développement le sont.

Il n'y a que trois approches possibles pour évaluer un actif : par les coûts – combien cela coûterait de reproduire les actifs ; les revenus – combien les actifs vont rapporter d'argent dans le futur ; par le marché – comment identifier des actifs comparables dans le marché ayant une valeur comparable.

La particularité des actifs incorporels est qu'ils sont souvent atypiques ou spécifiques. **Par définition, la plupart des actifs incorporels ne peuvent pas être évalués par l'approche de marché**.

IX.1.c. La valorisation des biens intangibles, une approche par les revenus pour les marques et les brevets.

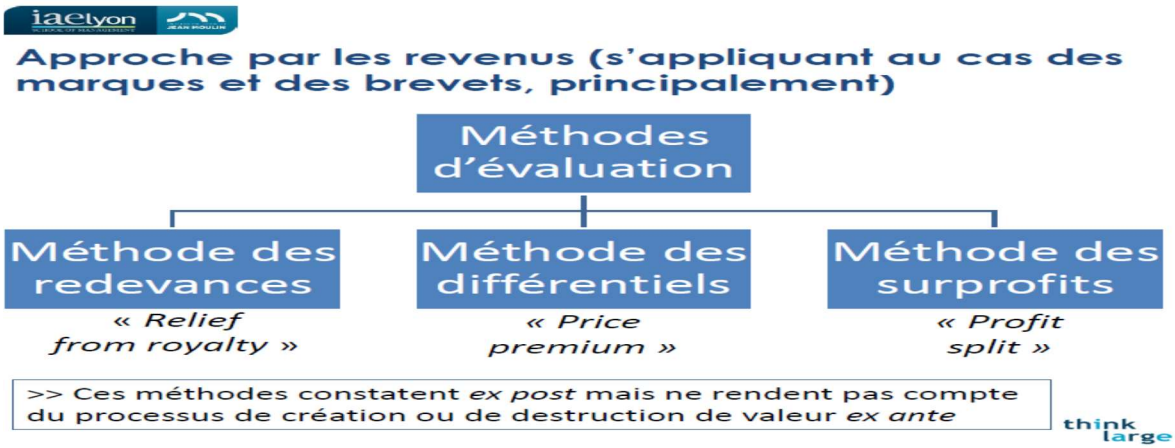


Figure 7 – Valorisation des biens intangibles

Les trois méthodes se déclinent en plusieurs techniques (trois ou quatre) en fonction du contexte, de la nature des actifs… La déontologie recommande l'utilisation d'au moins deux d'entre elles suffisamment différentes pour respecter l'impératif « multi critères ».

La méthode des redevances – *relief from royalties* : en étant propriétaire de la marque, on considère que c'est faire l'économie d'une redevance. À l'inverse, la marque pourrait être concédée à un tiers et il s'agirait de voir à quel taux de redevance, la marque en licence pourrait être concédée.

La méthode des différentiels – *price premium* : la prime de prix qui existe entre deux produits, l'un ayant une marque forte et l'autre pas. La différence implicite entre les deux donne la valeur de la marque du point de vue du client. Cette méthode est difficile à appliquer à cause du différentiel entre le prix d'achat et le prix consommateur. Il faut lever la marge du distributeur, les différentiels de qualité, de volume, de packaging et de publicité…

La méthode des surprofits – la règle du *profit split* permettra de considérer que sur ce sur profit, 30% sont, par exemple, attribuables à la marque.

Le normalisateur a considéré que ces méthodes ne sont pas suffisamment fiables pour être utilisées sur des actifs générés en interne. Mais elles le sont dans le cadre de regroupement d'entreprises lorsque le prix est capé par le prix d'acquisition global – le capital humain et les technologies pris en compte.

Une règle ISO définit les règles qui doivent être adoptées pour l'évaluation de la marque. Le point de vue financier doit ainsi prendre en compte les dimensions marketing et le juridique (suis-je ou pas propriétaire ?). En amont, les questions d'incertitude juridique sont présentées – ex. sous réserve de régularisation…, de titularité, date des dépôts, d'exploitation de la marque.

- **Le processus par lequel les marques acquièrent une valeur financière**

Le capital marque – un ensemble d'actifs et de passifs immatériels plus ou moins mesurés et contrôlés par le propriétaire de la marque et la marque – est un droit de propriété intellectuelle sur les bénéfices attendus du capital marque. La notion de valeur et de marque du point est différente du point de vue des clients actuels et de toutes les autres parties prenantes (salariés, fournisseurs investisseurs et société civile).

Les actifs et passifs du capital marque – *brand equity*, dans le capital marque ne peuvent se mesurer qu'au travers d'une mesure de la perception des clients par un recours aux techniques d'enquêtes et de sondages qui portent sur trois points : la connaissance de la marque – la notoriété, familiarité ; l'image – la qualité perçue, le caractère d'usage, les associations ; la loyauté – l'attitude et le comportement.

- **Le processus de création ou de destruction de la valeur d'une marque**

Il s'agit de comprendre les liens de cause à effet pour comprendre la construction et la destruction de valeur.

La valorisation financière est un constat. En revanche, les méthodes ne prennent pas en compte le processus de création de valeur qui passe par l'utilisation du **concept de capital marque** – *brand equity*. Le propriétaire de la marque contrôle la marque mais pas son capital-marque car la particularité de celui-ci est d'être située dans la tête des consommateurs. Or, on ne peut pas être maître de ce qui est dans la tête du client et pourtant l'entreprise, devant investir dans les actifs immatériels qui constituent ce capital marque, doit disposer des indicateurs financiers nécessaires pour investir afin de valoriser la marque.



Figure 8 – Valorisation financière

Les actifs immatériels ne sont pas maîtrisables mais ils apportent sans conteste de la valeur au consommateur client, valeur pour laquelle, il est prêt à payer. **La valeur d'utilité du client** découle de trois sources principales : la connaissance ou l'information – qui offre gain de temps ; la confiance et l'assurance – la marque garantie la qualité du produit, elle constitue une sorte d'assurance de nature informationnelle et anticipée, une sorte de « prime » ; l'émotion et la satisfaction – le sentiment de fierté qui est associé au produit. **La marque rapporte de la valeur au client, elle est une prime de prix.**

Si un risque cyber affecte l'image de marque, le processus de création de valeur et le capital marque sont affectés dans la tête du client. Certains actifs du capital marque ou d'utilité de la marque sont détruits et se transforment en passif. Même si le sinistre peut, dans certain cas augmenter la notoriété (par ex. le nom de la marque bénéficie d'une forte exposition médiatique), derrière se dégage une marge négative. Le passif est donc augmenté. Le client n'a plus confiance ou éprouve de la honte d'où une baisse consécutive de chiffre d'affaire voire de prix etc.

IX.1.d. L'assurance peut-elle assurer la confiance ?

La valorisation boursière est autonome par rapport à la publication des comptes de l'entreprise qui pourrait constater une baisse du chiffre d'affaire. Dans l'attente de la publication des comptes et de baisses de prix, les sondeurs pourraient mesurer en amont auprès des clients à quel niveau se situe le capital marque de l'entreprise (la connaissance, l'image et la loyauté). **Il faudrait pouvoir se poser la question de l'impact d'une attaque cyber entre indicateurs avancés et retardés**.

Dans le cas de *Yahoo*, est-ce que le risque cyber a été analysé dans le processus de *due diligence* ? Est-ce qu'ils ont pris en compte les mesures de mitigation du risque cyber ? En bourse en revanche, l'actif a été fortement déprécié.

Quels autres indicateurs utiliser sans passer par des sondages ? Des indicateurs paramétriques ?

Exemple de *Perrier* et l'incident du benzène en 1990, les assureurs ont payé les frais de retrait des bouteilles de *Perrier* pour conserver la marque.

Plus de de 80% de la valeur de la marque pour des groupes digitalisés est de l'intangible… Le risque cyber étant un risque qui affecte tout particulièrement la réputation de l'entreprise cela peut expliquer pourquoi l'on a si peu de retour d'information sur les entreprises qui ont subi des attaques.

Si l'on fait le ratio des actifs incorporels par rapport aux actifs corporels que couvre essentiellement l'assurance aujourd'hui, le potentiel de développement du marché pour couvrir l'immatériel est réel.

IX.2. Risque, audit et contrôle interne, l'organisation du management des risques dans la gestion d'entreprise et les documents obligatoires[54]

IX.2.a. Le management des risques, l'audit et le contrôle des risques dans les grandes entreprises – rôles et responsabilités

La typologie de « management du risque » dans l'entreprise couvre tous les types de risques opérationnel ou stratégique, développement commercial, de change, d'implantation, politique… Le management des risques, leur gestion, leur identification, leur analyse, la priorisation et le traitement sont normalement en adéquation avec la stratégie de l'entreprise. L'entreprise déploie un dispositif de gestion des risques.

- **Théorie**

Sur la base des souhaits d'évolution de l'organisation, l'entreprise procédera à l'identification, la priorisation et la réduction des risques. **L'audit et le contrôle interne contrôlent sur la base de ce qui a été identifié par le management des risques**. Elles s'assurent que les éléments de maîtrise de ces risques, qui ont été formalisés dans le cadre du management des risques, soient effectivement mis en place et suivis. L'audit interne fait le suivi du dispositif de contrôle et l'évaluation de l'efficacité. Il vérifie que ce qui a été analysé en termes de management des risques a été effectivement mis en place. Il est également appelé, la troisième ligne de défense.

- **Pratique**

Dans la pratique, ce mécanisme est bien implanté concernant le **champ du suivi financier du risque**. Il concerne également **la fraude réglementaire** – ne pas répondre ou suivre l'application des réglementations

[54] Présentation par *E&Y*. Voir https://www.ey.com/fr/fr/home

en place qui peut être identifié au niveau du management des risques, moins à celui de l'audit et encore moins en ce qui concerne la fonction de contrôle. **Sur la partie suivi du risque opérationnel et notamment cyber, l'exercice est balbutiant.**

L'interrogation porte sur les systèmes et la partie des comptes qui va être contrôlée et évaluée. Efficace et formalisée sur les éléments financiers, elle l'est moins sur d'autres risques opérationnels. **Aujourd'hui, l'audit et le contrôle interne manquent de connaissance sur le risque cyber pour l'évaluer. Le dialogue est rare et l'échange compliqué entre le directeur financier et le DSI par manque de structuration.** Il manque **la définition du système de norme et de procédure de contrôle, notamment les normes IFRS (*International financial reporting standards*), et la manière dont l'information va être captée et les fichiers qui vont être observés.**

La gestion des risques converge *in fine* avec l'information financière et comptable. On retrouve ainsi le *brand equity* au passif ou à l'actif des comptes de l'entreprise, certains risques peuvent être évalués d'autres non.

- **Comment s'opère la convergence entre les univers financiers et de gestion des risques ?**

Dans l'univers du management des risques, le risque est un aléa de toute nature – il peut affecter les marques, l'éthique ou le cyber … ; et ses conséquences sont diverses. **Les *risk managers* ou les assureurs vont s'intéresser à la nature de risques et à leurs impacts qui comportent des éléments négatifs pour l'entreprise par rapport à la valeur, sa stratégie, ses équipes etc**. Parallèlement, le gestionnaire de risque va également considérer le pendant positif du risque que sont les opportunités qui peuvent être manquées, non adressées et qui deviennent de ce fait des risques car ils ont un impact négatif.

La notion de risque, dans l'univers comptable et les règles comptable, est plus binaire. **Si l'on raisonne par analogie avec les provisions pour risque, la notion de risque devient une obligation probable pour l'entreprise vis-à-vis d'un tiers qui peut être évaluée de façon assez fiable et à une date de clôture donnée**. Un risque, comptablement parlant, est limité par ces critères. Un litige, qui a de fortes chances de se dénouer défavorablement à la clôture des comptes, va être inscrit au passif. Il va être reconnu comme un risque comptable et être enregistré comme tel à la clôture des comptes. En revanche, des risques liés aux marques, mais qu'on ne sait pas apprécier de façon fiable et qui n'est pas associable à un élément déclencheur précis, ne peuvent pas être comptabilisables.

- **Obligations résultant du RGPD et obligations de l'entreprise à l'égard des tiers**

Oui mais à condition que le fait soit avéré. Une entreprise peut identifier ses données dans le management des risques (ou une opportunité). Le fait que l'organisation puisse potentiellement être mise en responsabilité va être identifié et maîtrisé. Le fait que l'on ne soit pas sûr que les données aient été touchées ou pas, suffit à identifier, en termes de management du risque, que le risque a été réalisé **mais il ne suffit pas à l'identifier en tant que risque avéré au sens financier et comptable du terme**. **Un dépôt de plainte** et le fait qu'il y a une grosse potentialité de réalisation du risque et de jugement en défaveur de l'entreprise, peut en revanche être comptablement inscrit par l'entreprise. **Le commissaire aux comptes va prendre en compte cet évènement**. Si une entreprise décide de ne pas dévoiler un risque se traduisant par un litige probable et quantifiable, elle n'a pas intérêt à le faire apparaitre dans les livres de compte. **Les provisions sont généralement mises en place quand le risque est très avéré. Il y a une contradiction entre le management du risque et la traduction de ce même risque en termes comptables**. **La déductibilité fiscale des provisions est un élément se surajoutant aux premières considérations.** La provision pour être comptabilisée doit comporter un risque de sortie de ressource probable.

IX.2.b. Les critères de comptabilisation d'un risque au bilan sont restreints

Management des risques et état financier : l'évaluation des risques n'est, dans les comptes, que financière. **Seul l'impact financier, mesurable, quantifiable avec une bonne précision est retenu**. Par exemple, les difficultés pour recruter une équipe ne peuvent pas être provisionnées car elles ne peuvent pas se quantifier dans les comptes. On est limité par le fait qu'un risque au passif doit se traduire par une probabilité forte et une fiabilité suffisante de sortie de ressource financière. Pour que l'ensemble soit recevable par les commissaires aux comptes, **le système de contrôle interne de l'entreprise doit être conçu de manière à ce que les évaluations financières de ces risques soient fiables**. **L'évaluation comptable des risques en termes de réputation, de responsabilité pénale des dirigeants ou d'impact sur le business model sortent du cadre comptable**.

- **Les informations devant apparaitre dans les comptes et le bilan**

Pour les sociétés cotées, le **rapport aux actionnaires** décrit les risques dans un chapitre sur les facteurs de risque. La rédaction est libre. L'entreprise décrit ses différents facteurs de risque de manière littéraire et peu de chiffres sont demandés. **Peu d'entreprises ordonnent leur information de manière à dire d'un côté voilà le risque et voilà, en miroir, le dispositif de maitrise de risque mis en place et donc justifié**. **Ce paragraphe ne sert en aucune manière à évaluer ni la vulnérabilité d'une entreprise ni le risque considéré**.

Pour autant que les risques soient quantifiables comptablement, il existe une convergence entre les provisions pour risque comptabilisées pouvant toucher les garanties telles les remises en état à la suite des pollutions.

- **Une évolution nécessaire de la démarche de validation comptable des comptes**

Dans la démarche de validation comptable des comptes jusqu'à une époque récente, les dispositifs d'audit et de contrôle appuyaient le système de validation des comptes ainsi que l'intégration comptable d'exposition au risque éventuel dans le bilan final. **Ces outils d'audit et de contrôle n'ont pas été faits pour évaluer et quantifier notamment des risques opérationnels comme le cyber**.

Ceci étant, le risque environnemental fait l'objet désormais de provision pour risque pour des risques de pollution potentielle d'un site. Une vingtaine d'année ont été nécessaires pour mettre en place les indicateurs pour que ce risque soit formellement intégré dans la partie comptable.

IX.2.c. Comment amener les entreprises à structurer leur démarche ?

Au regard de la stratégie d'entreprise, le risque potentiel correspond à ce que l'entreprise expose en termes de risque en passant jusqu'à l'obligation probable, c'est-à-dire le risque effectivement réalisé, quantifiable, évaluable etc. et en cela intégrable et formalisable dans les comptes. **Il s'agit de rendre compte au conseil d'administration du niveau d'exposition aux risques via un recensement régulier de l'adéquation et de l'efficacité du dispositif de management des risques**.

L'objectif étant de valoriser le dispositif de management des risques dans la communication institutionnelle. Quatre étapes sont nécessaires.

Le conseil d'administration dispose d'un outil – une cartographie des risque qui lui permet de dresser un inventaire hiérarchisé, de disposer d'un outil de pilotage, définir des priorités d'actions et de mesure. Elle alimente les plans d'audit et donne des informations au comité d'audit.

- **Les points clefs de la cartographie des risques**

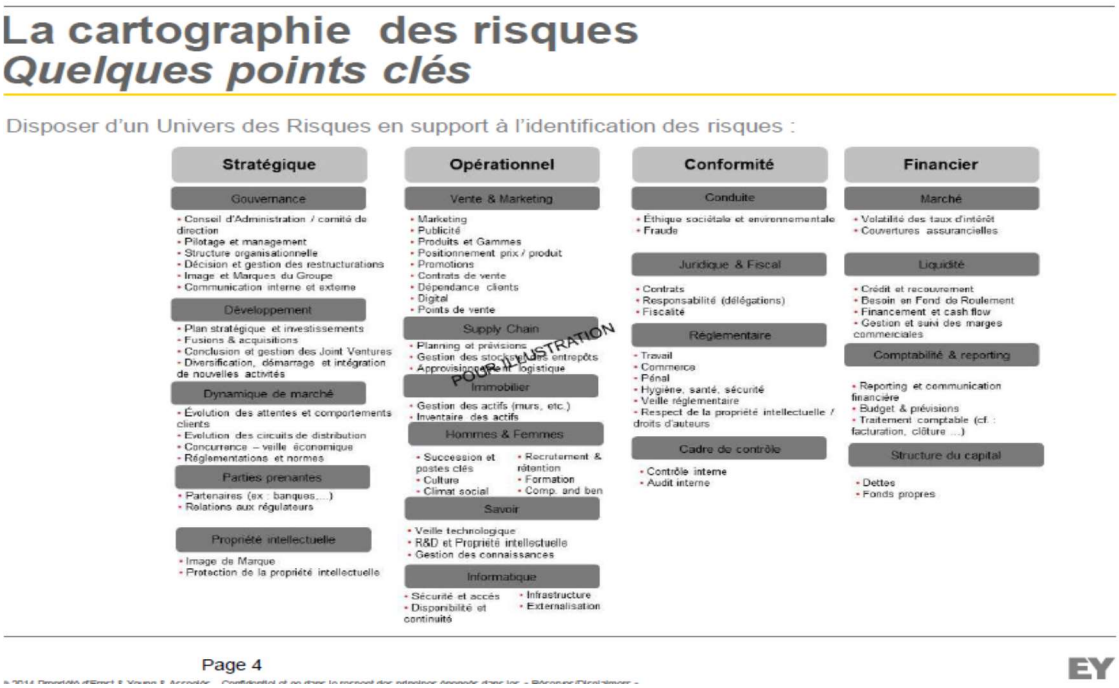


Figure 9 – Cartographie des risques

- **Les aspects qualitatifs de la cartographie des risques cyber opérationnels**

La cartographie est **renseignée qualitativement à l'aide de documents et d'éléments factuels** lors d'un atelier de travail avec la DSI ou le RSSI qui peuvent difficilement répondre autrement que positivement quant à la maîtrise de la gestion du risque cyber. **Les approches *top down* et *bottom up* sont croisées**. La fréquence de la mise à jour est à peu près tous les deux ans dans le meilleur des cas. **L'appétit au risque répond au choix entre risque, opportunité et finalité business**. Exemple : un SOC (*Security Operation Center*) risque de coûter en investissement et protection un tiers du chiffre d'affaire potentiel attendu. Sur les risques opérationnels, les éléments restent qualitatifs.

La formalisation de l'appétit au risque étant rarement faite, ces éléments factuels et qualitatifs permettent difficilement à un observateur extérieur de juger a posteriori des raisons qui ont présidé à la décision du conseil d'administration. Or ces facteurs démontrent la limite métier acceptée en dessous de laquelle le conseil d'administration s'autorise à prendre un risque. Et il est de sa responsabilité de prendre un risque pour saisir une opportunité business.

- **Deux contextes radicalement différents du fait de la régulation**

Réglementairement les règles de ***Solvency II***, imposent au conseil d'administration du secteur de la Banque et de l'Assurance de quantifier leurs risques. **C'est formalisé, obligatoire et justifié**. **Mais même dans ce secteur d'activité, si les risques financiers sont bien pris en compte, les risques opérationnels restent peu renseignés**. Sur les autres typologies d'entreprises, cela reste de la libre décision et justification du CA.

- **La détermination des indicateurs**

Après avoir procédé à l'analyse du risque, les indicateurs ont été déterminés en fonction de l'appétit au risque. **Il est du ressort du comité d'audit de suivre la mise en pratique et en application de ces dispositifs de maîtrise**. Le directeur de l'audit interne formalise les indicateurs qui vont permettre de suivre les avancements.

L'évolution constatée : de plus en plus de directions de l'audit interne cherchent à traduire dans l'approche d'audit la transcription et le suivi des risques opérationnels. **On voit apparaître la définition d'indicateurs de suivi des risques opérationnels dont le cyber**. Les comités d'audit commencent en effet à lister des bonnes pratiques en interne – les pratiques de l'ANSSI ou de l'ISO 27000, la bonne gestion des mots de passe, etc… Et des auditeurs internes suivent la mise en place de ces éléments dans l'entreprise. Un vrai progrès.

Il existe ainsi un gap important entre la partie identification, maîtrise et quantification du risque et la partie effectivement vue par le travail du commissaire au compte.

- **Validation des comptes, valorisation de l'intangible et assurance du point de vue du commissaire aux comptes**

Dans la démarche de gestion des risques, l'assurance va être située à la fin du processus après, l'identification, la maîtrise, l'analyse et ensuite le transfert. La théorie propose de suivre tout le processus de réduction et de ne transférer que le risque résiduel. **Les fonctions achat commencent à travailler sur la partie assurance et commencent à trouver des moyens de réduire les prix et vont sur une identification beaucoup plus factuelle de l'exposition aux risques**.

Les parties comptable et assurance poursuivent le même objectif mais obéissent à des logiques inversées. Du point de vue comptable, va être identifié ce qui est très probable. Un assureur n'assurera jamais un risque très probable sur le principe.

On retrouvera dans les captives, les caps d'évaluation et toute la difficulté d'évaluer le risque opérationnel. D'autant qu'un des problèmes de l'appétit au risque est de se situer sur les projets et les assureurs n'aiment pas assurer les projets.

- **Comment lire une cartographie des risques**

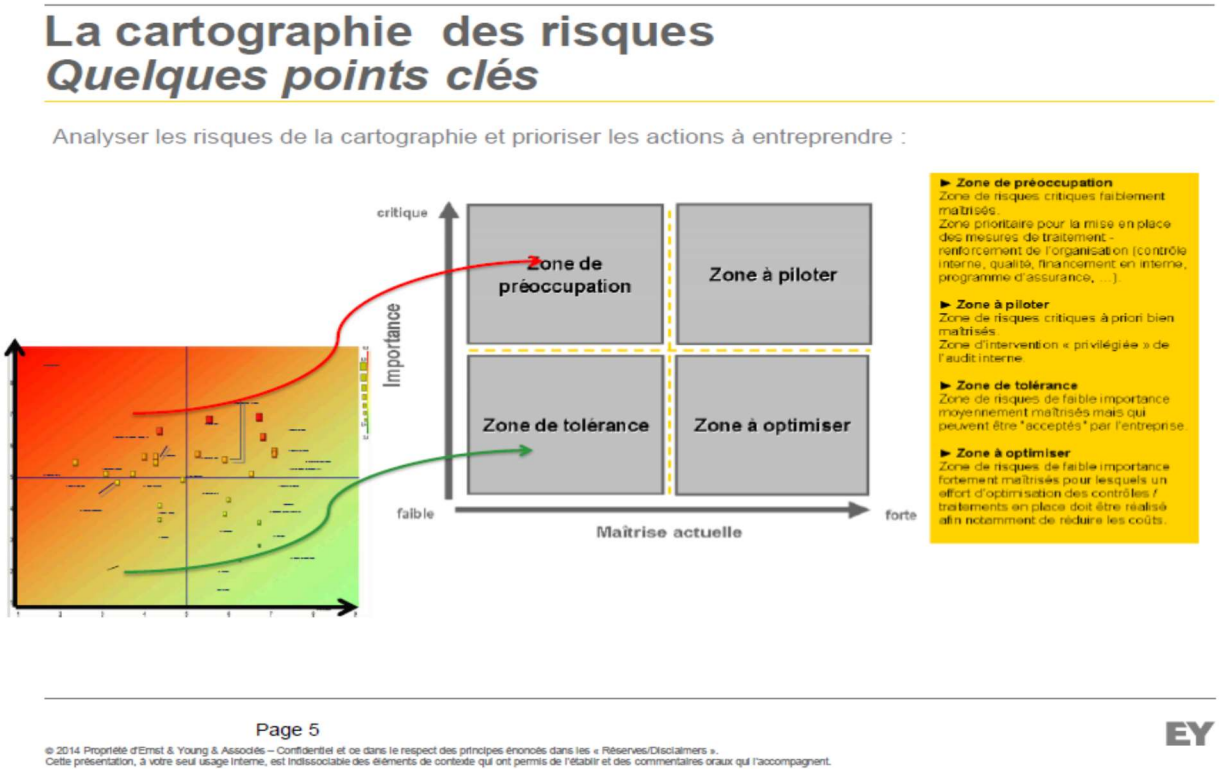


Figure 10 – Points clés d'une cartographie des risques

La cartographe des risques montre la maîtrise de la plus faible à la plus élevée ; l'exposition au risque de la plus faible à la plus élevée. Le risque est évalué, il est positionné dans la cartographie. La maîtrise est analysée de la manière la plus factuelle possible. Eventuellement, le risque est quantifié : global et factuel. Quand le risque se réalise, on est dans un dispositif de provision. L'écart entre les deux en termes de démarche est relativement grand.

Comment améliorer le rôle des commissaires aux comptes pour que le risque cyber apparaisse de façon plus factuelle dans le suivi et dans le bilan ? **Pour ce faire, il faut avancer sur la quantification financière du risque cyber. Il faut également rendre plus factuelle, la cartographie des risques**. Tant que cet exercice ne sera pas un exercice usuellement basé sur des chiffres et non pas sur de l'auto évaluation, il sera difficile de pousser une quantification du risque cyber comme celle d'autres risques.

De manière plus factuelle, dans la partie maîtrise du dispositif, faire dialoguer l'audit, le contrôle, la DSI, le RSSI pour d'identifier des indicateurs qui parlent à tous et soient reconnus par tous comme des éléments d'amélioration de la maîtrise. Concrètement, on en est aujourd'hui à travailler sur la maîtrise du risque cyber – un champ d'amélioration important, avant de travailler sur la quantification.

- **Les chiffres qui illustrent la cartographie**

L'évolution montre une prise en compte semi factuelle : des échelles sont proposées aux clients et sont ajustées avec eux.

Les critères habituellement partagés sont les suivants : **l'impact sur la stratégie**, **l'impact financier potentiel pour le client de la réalisation du risque** – en perte de CA ou de bid, l'impact sur les opérations – l'arrêt opérationnel, la partie réglementaire – mise en responsabilité administrative, civile ou pénale, l'image et le fait d'avoir une atteinte aux salariés aux tiers… Les grilles sont proposées aux clients et avec lui une évaluation semi factuelle est faite. Il arrive de plus en plus que de la quantification soit faite sur du risque très opérationnel.

Des formules relient les 5 ou 6 paramètres. Le principe n'est pas multiplicatif car l'objet de la cartographie est d'être une visualisation qui souhaite éviter de positionner tous les risques au centre du schéma. **L'échelle appliquée est généralement pilotée par le financier puisque c'est la conséquence financière qui est la plus aggravante**. Lorsque que différents risques sont cumulés, il va se situer de plus en plus vers le haut. Le principe est d'appliquer une échelle multiplicative mais pas linéaire mais logarithmique pour que les risques les plus patents apparaissent dans le rouge.

Il n'y a pas aujourd'hui de norme en la matière.

- **Comment positionner un risque non quantifié financièrement dans une cartographie ?**

Si la cartographie réunit les bons interlocuteurs, l'image du risque est réaliste. La quantification du risque va servir pour les risques les plus hauts afin de hiérarchiser la façon dont va être mis en place des éléments de maîtrise par exemple en montrant que l'interruption de business est évaluée à 300M€ alors que la mise en place d'un plan de continuité d'activité coûte 300K€.

- **Le rôle du régulateur sur le bilan des sociétés côtés**

Quel pourrait être l'*incentive* entre une entreprise qui met en place une véritable gouvernance du risque cyber, qui fait les investissements nécessaires pour l'analyse, la maîtrise et la quantification des risques par rapport à d'autres qui ne conduiraient aucune action dans ce domaine ? Rien n'apparaît sur le bilan des entreprises tant que ce bilan n'a pas eu lieu.

Actuellement, peu de réflexions sont menées entre le législateur et le régulateur pour obtenir une transparence qui pourrait avoir un impact sur la valorisation des entreprises. Pas de cadre existant. **Néanmoins, des pratiques existent notamment sur la justification**. Les cartographies des risques cyber sont utilisées par les investisseurs, dans le cadre de cessions d'entreprises. Le fait de démontrer un bon niveau de maîtrise ou pas et sa justification vont faire partie de la confiance qui va être accordée par les investisseurs. Mais quantifier financièrement la confiance de l'investisseur reste compliqué.

- **D'un point de vue réglementaire, il existe deux cas où la démonstration doit être faite en cas de problème, LPM (Loi de programmation militaire) et RGPD.**

La LPM dispose que l'organisation doit démontrer qu'elle s'est dotée des bons outils et des bons cadres d'évaluation et de gouvernance pour couvrir le risque. La LPM a moins été rédigée pour imposer des sanctions que pour développer des bonnes pratiques. Ainsi la partie amont : l'homologation est un élément pro actif qui vise à ce que les pratiques soient installées. **La finalité du règlement européen est différente dans le sens où elle n'est pas dotée de cet aspect amont.**

Le problème vient que le fait d'argumenter et de réunir les preuves sont un élément opposable en cas de réalisation du risque pour autant ils ne sont pas un élément de garantie avant que le risque se réalise.

IX.3. Le traitement par le juge judiciaire de l'indemnisation des préjudices immatériels[55]

La façon dont les juges judiciaires appréhendent la réparation des préjudices immatériels liés à l'économie numérique traduit une évolution similaire à celle qui a conduit la jurisprudence à admettre l'existence, à côté d'un principe de responsabilité pour faute, d'une responsabilité sans faute. La question qui leur est posée est de savoir s'ils ont bien pris la mesure des enjeux posés par les nouvelles technologies. On pourrait penser le contraire à la lecture de certains auteurs qui déplorent la faiblesse des dommages-intérêts accordés par exemple en matière de contrefaçon par les magistrats qui raisonneraient trop selon des schémas classiques. En réalité, si le principe de la réparation du préjudice immatériel ne pose pas de difficulté, c'est en revanche le contenu de celui-ci qui fait débats. C'est donc davantage la question de la preuve de ce préjudice qui se pose, ce qui rejoint ici aussi en matière judiciaire notre débat sur la qualification et la quantification de l'immatériel.

IX.3.a. Le préjudice immatériel et l'indemnisation. Principes

Le Pr. André Favre Rochex donne la définition suivante du préjudicie immatériel : « le **préjudice immatériel** cause à leur propriétaire ou leur utilisateur la destruction ou l'indisponibilité d'un bien indépendamment de la remise en état ou le remplacement de celui-ci ». Un **sinistre indemnisable** est constitué « d'un fait dommageable dont la conséquence a été d'occasionner un préjudice ».

Le **principe de la réparation intégrale du préjudice** rappelé tant par la doctrine que par la jurisprudence est le suivant : *«* Le propre de la responsabilité civile est de rétablir aussi exactement que possible l'équilibre détruit par le dommage, et de replacer la victime dans la situation où elle se serait trouvée si l'acte dommageable ne s'était pas produit *»*. Ce point est fondamental pour l'ensemble des juges français ou européens. **Toutes les actions qui seront entreprises pour respecter ce principe seront ainsi reçues par les juges à conditions qu'elles soient expliquées**.

Pour ce faire, il faut *«* replacer la victime dans la situation où elle se serait trouvé si l'acte dommageable ne s'était pas produit *»*. **Il s'agit d'établir la réalité du fait dommageable** ; **identifier les dommages**, ou chefs de préjudices, causés par ce fait dommageable ; et **s'assurer de l'existence d'un lien de causalité direct et certain** entre le fait dommageable et chaque chef de préjudice subi.

- **Deux points bloquants**

Les vraies difficultés à ce niveau sont l'évaluation du préjudice ainsi que la preuve du lien de causalité. Des pistes de réflexion existent.

IX.3.b. Le chiffrage du préjudice par le juge

Les préjudices immatériels sont les suivants :

- la désorganisation de l'entreprise ;
- le préjudicie commercial, le manque à gagner, la perte de marge, la perte de chance ;
- le préjudice moral et l'altération de la réputation ou de l'image.

Vincent Vigneau – Conseiller à la Cour de cassation déclarait au Colloque AFDIT en juin 2015 : « **… si le principe de la réparation du préjudice immatériel ne pose pas de difficulté, c'est en revanche le contenu de celui-ci**

[55] Présentation par Jean-Laurent Santoni (*CleverCourtage*) et Jean-Raymond Lemaire (*LCA-ICSI – expert judiciaire*).

qui fait débat ». Le magistrat explique que les dossiers qui lui sont présentés ne sont pas de « bonne qualité » dans la mesure où ils ne sont pas « compris » par les magistrats. Il faudrait en effet mieux expliquer en amont et présenter des éléments pour qu'ils puissent traiter de préjudice dans ces domaines techniques et nouveaux qui sont encore méconnus. **Il faut essentiellement de la pédagogie vis-à-vis du juge.**

Un important travail d'explication devra être ainsi produit lorsque les assureurs présenteront leurs premiers dossiers jusqu'en cassation. Il faudra accompagner, former et parler avec les juges. Lesquels sont demandeurs quant à ce qu'on attend d'eux dans ces domaines. Il faut ainsi **une réclamation claire, argumentée qui soit accompagnée d'éléments probants**. **Aucun formalisme n'est aujourd'hui imposé**.

De plus, les juges sont intéressés à ce que leur juridiction soit d'un bon niveau. Il existe une bataille très forte sur les problèmes d'atteinte à la marque dans le domaine du luxe. Paris a décidé de se doter d'un corps de juges de haut niveau pour pouvoir rivaliser avec les autres grands tribunaux européens notamment Francfort mais aussi Londres. La volonté d'exister à ce niveau est réelle de la part de la magistrature.

Paris pourrait-il ainsi se doter d'une spécialisation en cybersécurité ?

- **La charge de la preuve pèse sur le demandeur – l'enfer de la preuve.**

Le lien de causalité est un fait juridique, sa preuve peut s'administrer librement**.** Tout est recevable y compris faire appel à des experts judiciaires même lorsqu'ils interviennent dans le domaine privé puisque la cour de cassation reconnait que l'intervention d'experts privés de talent peut être suffisante pour étayer la démonstration – arrêt de la Cour de Cassation du 28 septembre 2012 : la nomination d'un expert est requise art. 145**.**

IX.3.c. L'évolution législative, vers l'élargissement de l'indemnisation des préjudices, l'exemple de l'atteinte au droit de la propriété intellectuelle. Principes.

L'objectif de la responsabilité au sens judiciaire du terme est – nous l'avons dit -, de « replacer la victime dans la situation où elle se serait trouvée si l'acte dommageable ne s'était pas produit ». Il n'est pas d'éviter que la victime ne le soit ou ne le redevienne. **La responsabilité civile a pour objet la réparation, pas la prévention.**

Dans de nombreux domaines, cette absence de caractère préventif ne présente pas d'inconvénient majeur, soit parce que des dispositifs complémentaires y suppléent efficacement, notamment la loi pénale, soit parce que le fait générateur de la responsabilité ne confère aucun avantage à son auteur, de sorte que la perspective d'avoir l'obligation d'indemniser suffit souvent à dissuader la commission d'un fait susceptible d'engager sa responsabilité.

En revanche, dans d'autres domaines, et tout particulièrement dans celui des dommages immatériels, le système de la réparation intégrale paraît manquer en partie son but. C'est le cas toutes les fois où le dommage ne survient pas fortuitement, on pourrait dire aussi accidentellement, mais résulte d'une action volontaire, dans le but d'obtenir un enrichissement en exploitant de façon illicite un droit de nature immatérielle appartenant à autrui.

Cela apparait avec encore plus d'acuité lorsque l'on prend en considération le fait que si le juge judiciaire se voit cantonner dans la simple réparation du préjudice sans avoir une action préventive, voir coercitive, il va abandonner ce rôle aux autorités administratives se sont emparées de la capacité à infliger des amendes administratives selon leur domaine d'intervention (CNIL, AMF, ACPR, …) à des niveaux de montants sans commune mesure avec les dommages-intérêts habituellement attribués (pour mémoire, les pénalités résultant de l'application du RGPD sont de 10 à 20 millions d'euros, et pour les entreprises jusqu'à 2 à 4 % de leur chiffres d'affaires annuel mondial).

Néanmoins, on observe une **évolution législative vers l'élargissement de l'indemnisation des préjudices : l'exemple de l'atteinte aux droits de propriété intellectuelle – Loi du 11 mars 2014, et l'émergence de la notion de faute lucrative et de la réparation des atteintes à des droits intangibles.**

Faire le lien avec les précédentes présentations montre que les valeurs immatérielles et intangibles étaient extrêmement importantes et si on reprend le schéma proposé par le Pr Chastenet sur la capitalisation boursière, les juges ne pourraient n'indemniser que la partie du graphique en rouge matérialisée dans les comptes. Et que tout le reste en bleu et vert intangible échapperait à l'indemnisation du juge. **Dans ce contexte-là, le législateur européen au travers de la directive du 29 avril 2004 inscrit dans le texte de la loi comment doit être appréhendé le principe de la réparation.** La réparation intégrale existe et on va plus loin désormais notamment dans le domaine de l'atteinte à la propriété intellectuelle. **C'est donc dans le domaine intangible que l'on voit poindre les modifications de la législation.**

Le juge doit appliquer et non inventer la loi. Si celle-ci dispose d'indemniser intégralement un préjudice clairement identifié, il ne peut pas réparer autre chose que ce qui est dans son pouvoir.

Il est intéressant de lire **que cette nouvelle écriture de l'article 331.1.3 du code de propriété intellectuelle stipule que pour fixer les dommages et intérêts, la juridiction prend en compte distinctement les conséquences économiques négatives de l'atteinte au droit dont le manque à gagner et la perte subie par la partie lésée mais aussi le préjudice moral causé à cette dernière**. Sont donc pris en compte les économies d'investissement intellectuel matériel promotionnel que celui-ci a retiré de l'atteinte au droit.

La **Cour de cassation** continue d'affirmer le principe du **Code Napoléon** qui veut que « la réparation ne peut excéder le montant du dommage » et que « les dommages-intérêts alloués à une victime doivent réparer le préjudice subi sans qu'il en résulte pour elle ni perte ni profit ». **Néanmoins une évolution** a été amorcée tant au niveau français qu'au niveau européen **pour faire évoluer les règles de réparation, tant en matière de prise en considération de la faute lucrative qu'en matière de réparation des atteintes à des droits intangibles (à défaut de définition des biens intangibles), principalement en matière d'atteinte aux droits de propriété intellectuelle**.

- **La faute lucrative**

La faute lucrative est la faute dont l'auteur retire un bénéfice supérieur au montant des réparations qu'il est tenu de payer, de sorte qu'il en tire nécessairement un avantage économique. Quand on a une pénalité de 150K€ au niveau de la CNIL par défaut de notification, faut-il mieux ne rien dire et risquer 150K ou dire et voir le titre s'effondrer ?

Cette faute lucrative se retrouve plutôt dans le domaine des atteintes à des droits intangibles, telles que les atteintes au droit de la propriété intellectuelle. **Il n'est pas illégitime de penser que la solution qui consiste à restituer à la victime les fruits de cette faute pourrait être étendue à toutes les atteintes aux biens intangibles, aux systèmes d'information et aux données**. Un tel mécanisme, qui aboutit à priver l'auteur de la faute de l'avantage qu'il en a retiré, serait de nature à décourager les atteintes réitérées commises de mauvaise foi dans des domaines où les conséquences profitables de cette faute ne sont pas neutralisées par la simple réparation des dommages causés.

A cet égard, on ne peut que regretter **que l'avant-projet de réforme du droit des obligations, qui se borne à reproduire à droit constant les articles 1382 à 1386-18 du Code civil, n'ait pas prévu de faire évoluer le droit positif sur ce point**. C'est pourtant ce qu'avait proposé le rapport Catala en septembre 2005, qui, tout en maintenant le principe de la réparation intégrale, proposait d'introduire un **nouvel article 1371** ainsi rédigé : « *L'auteur d'une faute manifestement délibérée, et notamment d'une faute lucrative, peut être condamné,*

outre les dommages-intérêts compensatoires, à des dommages-intérêts punitifs dont le juge a la faculté de faire bénéficier pour une part le Trésor public. La décision du juge d'octroyer de tels dommages-intérêts doit être spécialement motivée et leur montant distingué de celui des autres dommages-intérêts accordés à la victime. Les dommages-intérêts punitifs ne sont pas assurables ». **Voir Annexe 4 « Avant-projet de réforme du droit des obligations – septembre 2005 »**.

Dans cette perspective, force est de constater que si le juge judiciaire ne s'est pas vu attribuer la compétence à sanctionner l'auteur d'une faute lucrative, les autorités administratives se sont emparées de la capacité à infliger des amendes administratives selon leur domaine d'intervention (CNIL, AMF, ACPR, …) à des niveaux de montants sans commune mesure avec les dommages-intérêts habituellement attribués (pour mémoire, les pénalités résultant de l'application du RGPD sont de 10 à 20 millions d'euros, et pour les entreprises jusqu'à 2 à 4 % de leur chiffres d'affaires annuel mondial).

Il n'est pas impossible que le pouvoir revienne au juge judiciaire et que les textes évoluent.

- **La réparation du préjudice intangible**

Ce n'est pas tellement l'évolution législative vers l'élargissement à laquelle on assiste que **l'évolution jurisprudentielle vers la réduction de l'indemnisation des préjudices**. En particulier, plusieurs décisions sont intéressantes sur le fait « fautif » des victimes informatiques. Quand on regarde les pratiques jurisprudentielles on observe que les juges ont accepté de prendre en compte une évolution qui avait commencé en 1972 – arrêt portant des dommages corporels. La question étant, est-ce que le fait fautif de la victime diminue sa réparation ? Est-ce que cette logique peut être transférée dans les domaines matériels puis immatériels ?

C'est dans ce contexte que **la loi du 29 octobre 2007, transposant la directive 2004/48-CE du 29 avril 2004 relative au respect des droits de propriété intellectuelle, sans remettre en cause le principe de la réparation intégrale du préjudice, a néanmoins cherché à inciter les tribunaux, en matière de propriété intellectuelle, à prendre en compte, pour fixer les dommages-intérêts, non seulement les conséquences dommageables pour la victime de la contrefaçon, mais aussi celles bénéficiaires pour l'auteur.** La loi du 11 mars 2014, issue d'un rapport parlementaire d'évaluation de la loi de 2007, a renforcé ce mouvement.

L'article **L. 331-1-3 du Code de propriété intellectuelle** énonce ainsi désormais que, pour fixer les dommages et intérêts, la juridiction prend en considération **distinctement les conséquences économiques négatives de l'atteinte aux droits, dont le manque à gagner et la perte subis par la partie lésée, mais aussi le préjudice moral causé à cette dernière**. La juridiction prend également en considération les bénéfices réalisés par l'auteur de l'atteinte aux droits, y compris les économies d'investissements intellectuels, matériels et promotionnels que celui-ci a retirées de l'atteinte aux droits.

Ainsi, la victime peut obtenir l'indemnisation non seulement des conséquences économiques négatives causées par la contrefaçon que sont :

- **le manque à gagner**, c'est-à-dire le bénéfice dont le titulaire de droits a été privé, le gain qu'il aurait pu réaliser s'il avait été l'auteur des ventes contrefaisantes, lequel se calcule en multipliant la masse contrefaisante par le taux de marge du titulaire - le juge retient le plus souvent la marge nette du titulaire ;
- **les pertes économiques** subies par le titulaire de droits, c'est-à-dire la dévalorisation d'un droit exclusif, résultant de la qualité moindre des produits contrefaits, vendus à un prix inférieur et leur banalisation ;
- **le préjudice moral** résultant de l'altération de sa réputation ou son image ;

- **le bénéfice réalisé par l'auteur de la contrefaçon** ainsi que, depuis la loi de 2014, **les économies d'investissements intellectuels**, **matériels** et **promotionnels** que celui-ci a retirés de l'atteinte aux droits.

Ce dernier point est nouveau. Faisant application de la loi de 2007, **le TGI de Paris, dans une décision *Radioblog***, a ainsi condamné l'éditeur d'un site internet qui mettait à disposition du public sans autorisation des œuvres musicales, à verser aux victimes l'intégralité de son chiffre d'affaires, soit un total de plus de 1 million d'euros.

La partie recherche des brevets n'est pas reconnue comptablement ; seule la phase de développement l'est. Or, c'est cette phase qui est la plus coûteuse. Est-ce que, de leur côté, les juges peuvent recevoir la preuve des coûts de recherche ?

Le juge ne peut qu'appliquer la loi. Elle existe dans le domaine de la propriété intellectuelle et les marques pas pour les brevets. Sauf si on arrive à démontrer que le contrefacteur a réussi à économiser. Cela pourrait rentrer dans le cadre de l'indemnisation si on arrive à démontrer qu'en portant atteinte au droit des brevets ce dernier a fait l'économie de toutes les recherches. Dans le cas où la cible et le voleur ont été identifiés.

L'assurance couvre aujourd'hui les dommages causés à un tiers. Mais pas les dommages de risque opérationnels subis. On revient à l'hypothèse du risque pris par l'entreprise en fonction de sa stratégie business et l'assurance n'assure pas le risque d'entreprise car il n'y pas d'aléa.

IX.3.d. L'évolution jurisprudentielle vers la réduction de l'indemnisation des préjudices : le fait fautif des « victimes informatiques »

Depuis **un arrêt du 28 janvier 1972** le fait fautif des victimes est pris en considération pour l'indemnisation du préjudice, mais pour les seuls préjudices liés à une atteinte corporelle : « ***Cet arrêt avait considéré qu'il était légitime de réduire le montant des dommages et intérêts accordé aux familles de deux victimes décédées dans un accident de la route, au motif qu'elles avaient pris un risque en acceptant de monter dans un véhicule conduit par un chauffeur dont elles ne pouvaient ignorer l'état d'ivresse*** ».

Plus récemment le **21 février 2013, le TGI** de Paris s'est prononcé dans **l'affaire *Sarenza***. Cette entreprise de e-Commerce cyber-attaquée par un collaborateur a obtenu la condamnation du responsable de la cyber-attaque par le TGI de Paris à une hauteur de 100.000 euros mais le même tribunal a pris une autre décision. **Le tribunal a estimé que la société était responsable de son propre préjudice à hauteur de 30% en raison de son « manque de rigueur » dans la gestion des identifiants**. Pour rappel, ce site de e-commerce gère un fichier de 4,7 millions d'adresses électroniques de clients et prospects. Le TGI a estimé qu'il manquait à *Sarenza* un bon niveau de sécurité et de contrôle. **La victime a été jugée comme ayant contribué à la réalisation de son préjudicie en sécurisant de façon insuffisante l'accès aux adresses électroniques de ses clients et prospects qui avaient été détournés**. La victime fait état de son *data breach* et repart avec un **226.17** en tant que responsable d'un défaut de sécurité. Quand on demande réparation, le juge répond qu'il y a une part pour la victime co-responsable du dommage.

De plus, dans **la jurisprudence Kerviel du 9 mars 2014**, la chambre criminelle de la cour de Cassation **semble également démontrer que les juges tiennent de plus en plus compte de la qualité et du niveau des cyber-protections et de leurs fonctionnements via le respect des procédures internes dans ce type d'affaire**. Elle a rejeté dans sa formation plénière le pourvoi de Jérôme Kerviel concernant les dispositions pénales en disant que Kerviel est pénalement répréhensible en application de la loi Godfrain mais elle a réformé l'arrêt de la cour d'Appel sur les dispositions civiles sur les 4,9 milliards que devait payer J. Kerviel à la Société générale correspondant à l'entier préjudice de la banque. La cour d'Appel s'était appuyée sur un certain nombre de

fautes commises et sur les décisions de l'AMF, de la Commission bancaire de 2008. Les 50 milliards d'euros de positions prises par Jérôme Kerviel entre le 3 et 18 janvier ne peuvent pas être passées inaperçues. Comment identifier les défaillances de la banque ? « ***il est vrai qu'au niveau du système Eliot il n'existe aucun contrôle qui serait de nature à alerter sur une saisie incohérente dans la mesure où les champs obligatoires sont renseignés*** »; c'est ce que l'on peut lire dans l'arrêt de la cour de Cassation daté du 19 mars 2014. On y trouve aussi « ***l'ensemble de sa hiérarchie et des services de contrôle savaient mais l'avaient laissé faire à raison notamment de leur inertie face aux différents indicateurs d'alertes internes ou extérieures*** ».

Il est en effet apparu que la cour d'appel, après avoir relevé l'existence de fautes commises par la *Société Générale* ayant concouru au développement de la fraude et à ses conséquences financières, n'a pas tenu compte de ces fautes pour évaluer la réparation du dommage mise à la charge du prévenu.

- **Comment éviter de se retrouver fautif lorsqu'on est victime ?**

Au-delà des « affaires »*Sarenza* et *SocGen*, **le comportement des utilisateurs des ressources IT au sein des organisations soulève trois points**. Le comportement est visé en termes de **co-responsabilité**. La Chambre criminelle fait ainsi évoluer la jurisprudence de la Chambre mixte du 28 janvier 1972, la jurisprudence des chambres civiles et de sa propre jurisprudence relative aux infractions volontaires et involontaires contre les personnes, selon lesquelles, **lorsque plusieurs fautes ont concouru au dommage, la responsabilité de leurs auteurs se trouve engagée dans une mesure qu'il appartient aux juges du fond de déterminer**. Ainsi, quelle que soit la nature des infractions commises aux personnes et aux biens, les juridictions pénales qui constatent l'existence d'une faute de la victime ayant concouru au dommage, sont amenées à en tirer les conséquences sur l'évaluation du montant de l'indemnité due à cette dernière par le prévenu.

L'assureur peut être intéressé par cette décision car elle pose la question de l'indemnisation de l'assureur du dommage causant un recours contre l'auteur.

Il s'y ajoute que **la jurisprudence du Conseil d'Etat interdit la déductibilité d'une provision fiscale pour compenser une partie des pertes subies en cas de responsabilité de la part de l'établissement concerné** (pour mémoire c'est 1,7 milliard d'euros, consentie en 2008 par Bercy pour compenser une partie des pertes imputées à J. Kerviel).

Peut-on aussi considérer que l'assuré « victime informatique » de son défaut de sécurité mis en évidence par une Autorité de Contrôle verrait remise en cause l'indemnisation de son préjudice par l'assureur, une sorte de « règle proportionnelle d'indemnisation » ? Après la règle proportionnelle de capitaux resterait à inventer la règle proportionnelle de taux de prime. Une vraie question se pose.

IX.3.e. La préparation du traitement judiciaire commence avant la crise

Un maximum d'éléments doit être préparé avant la crise qui doit réunir tous les acteurs. Ce moment-là doit être extrêmement bien géré par un chef d'orchestre. Il faut que les référentiels qui serviront à établir le préjudice soient préparés à l'avance pour être plus convainquant si nécessaire devant le juge.

Il faut l'avoir préparé pour ne pas prendre à chaud des décisions et des indicateurs et pour ne pas avoir à travailler a posteriori sur la compensation par un préjudice qui sera demandé à l'assureur et ou à un juge. Les mécanismes de réflexion et de mise en œuvre sont les mêmes.

- **Des mécanismes d'assurance paramétrique, une solution ?**

Dès lors qu'ils sont préparés et que les paramètres sont fondés, ils pourraient plus facilement entrainer la conviction de l'assureur pour couvrir le risque et du juge en cas de litige. Les dispositifs de gestion de crise sont essentiellement orientés vers de la réponse technique, SOC – CERT. Les courtiers se sont raccrochés à des

opérateurs techniques en ne prenant pas en compte la dimension juridique et le traitement judiciaire. Seules ont été pris en compte, les dimensions relation avec les autorités administratives qui ont supplanté le juge judiciaire. Mais ce dernier reviendra à la charge face à cette perte de leurs prérogatives face aux autorités administratives dans les parquets financiers et autre *pop* droits à l'américaine.

Tous ces éléments vont devoir être formalisés. Il faudra propager cette information et former les prestataires et avocats.

- **Assurance paramétrique et paramétrisation des biens intangibles**

Il ne faut pas attendre que la comptabilité change. On ne pourra jamais inscrire les passifs de l'immatériel. La dernière réglementation internationale date de 2005 (cf. l'IAS 38 et les normes IFR). Il résulte d'un consensus international difficilement modifiable[56]. En revanche, **rien n'empêche un Groupe d'essayer de quantifier et de tenir une comptabilité double extra financière** pour commencer à quantifier son capital marque et commencer à identifier des mesures de notoriété tous les six mois selon un processus qui va être de moins en moins couteux car réitéré et optimisé. Et le jour où il y aura une attaque sur la marque, on verra bien qu'il y aura eu durant six mois une baisse de notoriété avec la raison associée.

Cette double comptabilité peut être reçue par le juge si l'on montre que c'est quelque chose qui a une fiabilité dans la quantification du phénomène. Ceci devient un fait juridique qu'on a la possibilité de prouver. Il ne faut pas le faire le jour de la crise.

L'assurance paramétrique peut donc s'envisager.

- **Comment matérialiser l'atteinte à l'image ?**

Comment estimer l'effort financier de « réparation » de l'image et évaluer le préjudice subi du fait de l'altération de l'image ? **La matérialisation de l'atteinte à l'image est possible si des indicateurs objectifs, quantifiables, permettent de « mesurer » régulièrement cette image**. Citations dans les médias, sur les réseaux, … cours de bourse, … messages positifs, neutres, négatifs. **Cela se prépare**.

Une détérioration de l'image peut être alors mise en exergue. Un plan d'actions avec des moyens et des objectifs peut être chiffré. Si des pertes de part de marché, de contrats, des détériorations de conditions financières … suivent, il faut alors essayer de définir le lien de causalité. **Tout ceci nécessite anticipation, préparation et pour les référentiels une décorrélation de leur création et de la crise.**

- **La responsabilité des acteurs face aux bombes logiques**

La question de la date de déclenchement pose celle de la personne qui déclenche et sa responsabilité directe. Dans cette perspective, c'est difficilement opposable à la société. C'est non auditable surtout quand c'est du code compilé. Il y a également des processus : vérifier que l'on dispose des codes sources, que les mises à jour ont été faites.

[56] Néanmoins, la Stratégie de Cyber défense de 2018 propose que la France soutienne une évolution de la régulation internationale dans ce domaine. Voir tableau du suivi des recommandations – Annexe 10.

X. La réponse de l'assurance (et de la réassurance) pour couvrir les biens tangibles et intangibles

Verrous

Pour le marché de l'assurance, quelles sont les informations nécessaires pour la prise en compte des biens intangibles ? Comment désormais gérer la souscription ? Les sinistres ? Peut-on envisager une évolution de l'offre ?

Comment adresser l'enjeu de la faiblesse des capacités financières actuellement disponibles sur le marché ?

Comment faire pour rassembler les capacités nécessaires pour que le recours à l'assurance ait du sens ?

X.1. Première étape : sécuriser les nouveaux produits d'assurance cyber

À la suite des présentations de ce qu'est un bien intangible et ses possibles valorisations, la FFA et l'APREF se sont réunis par trois fois pour traiter ce sujet. La profession témoigne avoir d'autres challenges concernant le risque cyber à résoudre avant de traiter le transfert des risques intangibles.

X.1.a. Retour d'expérience sur la mise en place de programmes d'assurance cyber à vocation de masse[57]

Nous partageons ici **un retour d'expérience** sur la mise en place de programmes cyber dont la vocation était d'avoir des contrats à vocation de masse sous l'égide d'un réassureur et en accompagnement d'une cédante à la mise en place d'un contrat d'assurance dédié pour des professionnels ou des TPE et également un produit sur mesure. Deux approches qui ont chacune leurs avantages.

- **Exemple d'approche dédiée sous forme de gamme : produits Pro et TPE standards et produits sur mesure**

Exemple d'approche dédiée sous forme de gamme : produits Pro – TPE standards et produits sur mesure

Exemple d'approche intégrée sous forme d'extension cyber d'assurance, une police groupe RC Pro

Une approche sous forme de gamme : produits dédiés

Le challenge était de réaliser une exploration pour un réseau d'agences d'un assureur généraliste : le GAN d'une offre cyber qui réponde à **trois objectifs** – **simple à vendre**, **facile à souscrire** pour des risques de base et **dont l'indemnisation soit efficace**. Une offre qui puisse être opérationnelle dans le cadre de la relation avec le client. Le choix s'est porté sur un découpage en deux offres – standard et sur mesure :

1. **L'offre standard** est une offre standard pour les entreprises et les professionnels réalisant moins de 1M€ de chiffre d'affaire soit 70% du portefeuille. **Le principe était d'abandonner le principe du questionnaire de souscription** mais d'avoir **une approche mettant en place des conditions d'octroi de la garantie** faisant référence au guide d'hygiène de la sécurité des systèmes d'information de l'ANSSI dans sa première et seconde version. **Une prise de garantie immédiate** dès que le bulletin de souscription est complété, signé et daté.

[57] Présentation de Jean-Laurent Santoni, *CleverCourtage*.

Une plateforme pour porter assistance car l'approche consistait à dire : le jour où il y a un évènement matériel ou immatériel au système d'information, **il s'agissait de pouvoir répondre** à la première question posée à savoir « qu'est ce qui s'est passé ». Le montage a été d'abord fondé sur **une approche gestion de crise** afin de pouvoir immédiatement **à la qualification de la situation**. La victime appelle la plateforme. L'interlocuteur demande ce qu'il arrive et évalue avec le client **si l'évènement est éligible à l'assurance**. Ce point est majeur. Il s'agit de ne pas déclencher le mécanisme d'assurance et d'indemnisation sur des évènements qui seraient des problématiques de maintenance, d'erreurs… et pas cyber. Cette problématique de qualification est systématique. **Le calcul de la prime a pris en compte le temps de la gestion de la crise**. Car si ce dernier est bien pris en compte, **en règle générale, l'ensemble des frais est limité dans ses volets dommage aux biens**, **décontamination**, **reconstitution** et **frais complémentaires**. Et cela limite corrélativement la mise en cause de la responsabilité civile car dès le début on arrive à gérer la problématique en la qualifiant et la traitant. La détermination des critères d'éligibilité n'est pas si aisée.

La plateforme d'assistance est ouverte 5 jours sur 7 en 2017. Elle le sera 6 jours sur 7 en 2018. La plateforme fonctionne sur la partie standard et sur la partie sur mesure. La plateforme a été conçue pour amener directement une réponse.

Le montage de la garantie est une combinatoire RC et Dommages à capital global car on ne se sait pas a priori si l'évènement sera constitutif d'une problématique de responsabilité civile ou de dommage. Il se peut qu'il faille débloquer une situation technique. Cela serait peut-être ou cela sera : c'est une problématique de responsabilité dans laquelle il y aura des mises en causes. Le volet est attribué en fonction du besoin.

Le projet visait une garantie standard globale d'engagement de 150K€ : 50K€ de gestion de crise et 100K€ de garantie combinée RC Dommages qui ira selon la nature de l'évènement vers un mécanisme de frais ou de pertes indemnitaires. Le montant de la prime étant de 500 ou 550€ TC. L'essentiel de la prime vise à aider à la garantie de gestion de crise.

Les évènements couverts dans la garantie de base sont **l'atteinte au système** et **aux données entrainant des frais et ou générant des pertes**. Les évènements ne couvrent dans la partie dommage que les frais de contamination internes ou externes. Les aspects erreurs ne sont pris en charge que dans la garantie sur mesure. La garantie est expliquée dans l'objectif de créer de la relation avec le client d'expliquer et faire du service.

2. **La garantie sur mesure a été faite pour des entreprises ou des professionnels quelques soit leur chiffre d'affaire. La garantie cumulée permet de jouer entre un peu plus de RC, un peu moins de Dommage sur la base d'une analyse du besoin du client.**

Selon une approche de profilage du client. **Le questionnaire utilisé n'est pas un questionnaire de la sécurité mais de profilage de l'activité utilisant les moyens et les systèmes d'information**.

Autrement dit, l'analyse se fait **en fonction de la nature de l'activité** – ex. un hôtelier qui fait de la réservation sur internet en utilisant des cartes bancaires et collecte des données personnelles – un expert-comptable qui gère la paye pour le compte de ses clients …. Ce profil de risque est totalement indépendant d'éléments techniques du SI, de l'utilisation d'un prestataire de Cloud etc.

L'intérêt de cette approche n'est pas de s'occuper du risque à l'informatique mais du risque de l'entreprise informatisée. Cela rejoint l'approche SPICE en disant : ce n'est pas un problème informatique mais c'est un problème d'utilisation d'un système d'information en fonction de son activité. Le profil d'un avocat sera différent de celui d'un médecin, d'une activité de fabrication de produits ou d'une activité de services, etc.

Parmi les questions du profil, des questions portent sur : « **de qui dépendez–vous**, quels sont les éléments partagées ». **Ce qui permet d'agréger dans le portefeuille tous ceux qui** par exemple sont hébergés chez le même opérateur de cloud ou le même hébergeur (exemple d'OVH), tous ceux qui utilisent Office 365 ou la même messagerie, tel et tel moyen.

Car en agrégeant l'ensemble des moyens on se trouve dans une configuration de *supply chain* et on connait l'ensemble des acteurs qui si ils vont connaître une défaillance vont avoir un effet ricochet à l'intérieur des profils considérés. **Cela permet de régler l'une des problématiques majeures pour l'assureur qui n'est pas son exposition unitaire mais son exposition systémique**. **Le vrai sujet est quel est votre profil de business et quelle est votre degré de dépendance vis-à-vis de votre activité.**

Dans cette approche-là, les garanties sur mesure incluent dans le volet RC, les mises en cause suite à une atteinte à la propriété intellectuelle, à la vie privée, au droit à l'image, les mises en cause sur les agissements diffamatoires, les publicités mensongères. Dans le volet Dommage sont pris en compte les dommages aux biens et les reconstitutions suite à une erreur humaine. Lors de l'établissement du profil, il aura été répondu aux questions est-ce que c'est vous qui développez, est-ce que les éléments sont testés : tous les éléments de maturité. Dans ce cas-là, l'analyse du profil est conduite de façon plus approfondie.

La partie perte d'exploitation est prise en compte également dans le sens perte de marge brute. Des passerelles ont été faites avec les polices dommages, perte d'exploitation, RC pro et polices fraudes dans une cohérence globale qui a mis en lumière un besoin d'amélioration de cohérence par rapport aux autres programmes. A partir de là, le capital de gestion de crise peut maintenir une combinée RC.

Un système de calcul permet de dire lorsqu'on arrive à un total d'1M€, c'est l'entité souscriptrice qui gère et au-delà de ces seuils il y a une relation avec le réassureur s'il y a besoin d'aller sur des métiers particuliers ou des agrégations de capitaux.

3. **L'accompagnement à la vente. Un effort important a été conduit par l'assureur sur l'accompagnement à la vente en faisant le pari de fournir aux agents la compréhension de ces risques.**

Le premier groupe d'agents d'assurance formés ayant été les « geeks » du département qui étaient intéressés par la vente de ce type de produits parce qu'ils maîtrisaient les nouvelles technologies et parce qu'ils étaient intéressés à pénétrer un nouvel environnement concurrentiel.

Un effort d'accompagnement important a été fourni sur **les conditions générales**, les guides de profil, les différents processus de souscription en sur mesure et standard, les outils de consolidation, les nuages de point pour voir les différents domaines, les plaquettes, les FAQ (remise en forme de toutes les questions venant du terrain pour les rendre intelligibles et repartagées) pour créer un dialogue. Cette notion de profil a été bien appréhendée car elle permettait de se décentrer de l'approche technique pour poser des questions orientées métiers : comment l'hôtelier utilise les moyens de paiement, comment vous collectez des données sensibles…

4. **Des conditions de souscription simplifiée. Pas de questionnaire sur la garantie standard**

Le questionnaire de profilage est conservé pour la seule garantie sur mesure. Cette absence de questionnaire a permis de faire une classification par rapport à des codes APE NAF et d'avoir une visibilité sur des portefeuilles existants pour rajouter une garantie en extension de l'existant sur le cyber. Cette approche permet de créer un socle cyber avant d'aller sur une garantie sur mesure de deuxième ligne qui permet d'affiner. Dans les conditions d'octroi ont été retenus trois grandes règles que sont la sauvegarde, l'antivirus et la gestion des pare feux.

Pour la garantie sur mesure, et la problématique des erreurs ont été rajoutés dans la garantie d'octroi les tests de logiciels quand ils sont développés en internes. Concernant la garantie perte d'exploitation, une condition modeste de plan de secours a été rajoutée – une description de l'organisation de l'entreprise pour que la garantie PE prévue pour une indemnisation de 3 mois permette une vraie efficacité.

Il est stipulé que la condition d'octroi ne s'exerce pas s'il s'avère que le dommage est sans relation avec la condition.

Le marché montre une diversité de situations dans les règles d'indemnisation. La sanction du non-respect d'une condition d'octroi peut être le refus de garantie. D'autres considèrent que c'est l'application d'une franchise plus élevée. Néanmoins, **cela permet de demander un minimum d'hygiène informatique**.

5. **Un questionnaire de profilage pour une garantie importante**

En revanche, le questionnaire de profilage nécessaire une demande pour une garantie d'1M€ a été construit autour de deux objectifs : l'évaluation de l'exposition au risque de l'assuré afin de déterminer le niveau de tarification applicable ; et l'évaluation au risque de l'assuré pour l'aider à identifier ses garanties correspondantes à ses besoins de couverture.

Le dialogue assureur assuré est dépassé pour entrer dans un dialogue de quasi conseil : « par rapport au profil qui est le vôtre, par rapport à nos analyses et votre business, vous devriez avoir tel type d'exposition telle et telle volumétrie et être proche de telle catégorie. Si vous êtes proches de cette catégorie, c'est une aide à la décision. Si vous êtes éloignés, c'est une aide à la décision pour comprendre votre différence. » On retrouve là d'autres éléments que sont **l'activité**, **le chiffre d'affaire**, **le niveau de franchise**, **le nombre d'enregistrement des données tenu pour l'activité** (cf. le RGPD) pouvant servir à la fois pour les aspects notification et les aspects de volume d'activité.

Les approches de profil ressemblent à des politiques de sécurité. Cet outil de profilage a une vertu unitaire d'expliquer dans le dialogue entre l'assureur et l'assuré, entre l'agent et l'assuré le besoin par rapport au profil et quel type de garantie on peut mettre en place. Il permet de mettre en évidence le niveau de garantie pour lequel il n'y a pas de réponse.

Vis-à-vis de l'entité, **cet outil de profil permet d'agréger les cumuls d'exposition**, **de remonter les informations permettant de s'apercevoir sur l'ensemble du portefeuille quels sont les assurés qui hébergent leurs données**, **utilisent tel type de système**. Cela permet ainsi d'identifier un certain nombre de points d'analyse sur lesquels il y a un éveil à avoir en matière systémique.

6. **L'indemnisation efficace se fait via la plateforme de gestion de crise et de sinistres.**

Une phase de réaction à chaud technique avec une dimension juridique de ne pas détruire les preuves.

En phase de crise, pour résoudre les problèmes, l'intervenant technique est souvent celui qui est intervenu comme opérateur du client. D'où la difficulté, le cas échéant, de conserver des preuves pour des recours éventuels.

Ensuite viennent les analyses à froid, la décontamination, avec des aspects de recommandation. Puis se pose la question de la recherche des responsabilités. L'assureur bénéficiant d'un recours subrogatoire vis-à-vis de l'auteur final, l'expert judicaire intervient, le lien avec la CNIL est fait, la question de l'indemnisation des tiers est abordée, celle des recours contre les fournisseurs, les hébergeurs est posée… Un numéro vert gratuit est à la disposition des assurés. Le retour sur la plateforme que font les différents acteurs, dont les agents et les assureurs est positif. Ils expriment un soulagement. Ils reconnaissent que la qualité de la relation permet de

calmer le débat, d'identifier les problématiques, qu'en l'espèce il ne s'agit pas forcément d'une problématique cyber et enfin de protéger la police d'assurance.

Il s'agit ici du choix d'un assureur qui souhaitait avoir une police dédiée s'inscrivant au milieu de ses problématiques dommages, responsabilité et répondant, au travers de son réseau d'agents, à une problématique de relation et de positionnement sur le marché français. Le groupe auquel appartient cet assureur étant attentif au succès de cette première phase de mise en place.

- **Une approche intégrée sous forme d'extension de police cyber sur mesure une police RC pro**

Deux illustrations du marché ont été étudiées : une police groupe de dommage (voir la police de dommage du *Syntec numérique*) et la police RC pro groupe d'une profession réglementée – celle des Experts comptables. Cette police est soumise à des règles prudentielles professionnelles sur la protection des données des clients – salaires, accidents de travail …. Il s'agissait de prendre en compte la possibilité que leur système d'information puisse faire l'objet d'une passerelle dans le cadre de la dématérialisation de leurs échanges – les virements des salaires à l'Urssaf, aux caisses de retraite.

La réponse apportée aux enjeux de cette profession fut de « première ligne », une intégration dans la police globale d'une garantie de gestion de crise à hauteur de 50.000 euros. Une garantie perte de données à hauteur de 120.00 euros sans franchise associée à d'autres garanties de frais supplémentaires, frais de notation de 20.000 euros. Tout ceci est compris dans le package de la garantie globale de groupe intégrée dans la RC pro.

Les conditions de garanties sont assez drastiques réunissant des conditions d'octroi, des réseaux sécurisés, des logiciels utilisés selon les recommandations de l'éditeur, un anti-virus, la condition de sensibilisation des employés du cabinet et enfin les ordinateurs portables devant détenir un système de chiffrement intégral permettant de sécuriser le disque dur.

La garantie de base pouvant être nécessaire mais pas suffisante, la police de groupe a rajouté trois options en troisième ligne : 50.000 euros, 100.000 et 200.000.

Ce produit est intégré bien que la tarification soit réalisée à part avec des options séparées.

- **Conclusion**

Deux possibilités entre produits cyber intégrés ou dédiés ? Quel référentiel et quel suivi des engagements ?

L'ensemble du marché des assureurs s'est initialement focalisé sur les grands comptes et s'est prononcé en faveur d'une option cyber dédiée selon un modèle anglo-saxon. L'option est réaliste à la condition que le produit soit dimensionné pour apporter une réponse adaptée à ceux pour qui il est adressé. Le choix du GAN a d'abord été en faveur **d'une garantie de gestion de crise forte pour permettre de limiter l'exposition en dommage ou en RC par la bonne qualification de la situation et une réponse rapide. Tout le monde peut assurer, mais qui peut vraiment répondre rapidement et qualitativement ?**

L'approche choisie en l'espèce est **d'abord l'assistance et ensuite la garantie intégrée** qui s'adresse plutôt à soit un portefeuille existant permettant à un assureur d'en garder la maîtrise – une extension d'atteinte aux systèmes et aux données par une cause immatérielle dans une police de dommage. **Ou une garantie en RC dans laquelle on rajoute une garantie des tiers lésés résultants d'une atteinte au système et aux données**. Cela conduit à proposer une garantie élargie souvent une pollicitation de garanties existantes. **L'assureur ayant un début de polices d'assurance cyber nécessairement limitée en garanties de capitaux mais cela lui permet de maîtriser son exposition, de répondre à la problématique des couvertures silencieuses, de recueillir de la prime, de se protéger contre une interprétation extensive de la police de base si elle n'est pas suffisamment précise**. L'imprécision du texte d'une police de base peut en effet avoir pour conséquence

une interprétation en tant que police cyber. Il vaut mieux, dans ce cas, avoir une extension clairement déterminée. Une solution claire pour un assureur qui souhaite protéger son portefeuille.

X.1.b. La stratégie du Lloyds de Londres pour l'assurance du risque cyber[58]

- **Les points clefs du marché du Lloyds[59] et son fonctionnement**

Lloyds de Londres est une plateforme dans laquelle les investisseurs – dont les membres sont gérés par les *managing agents* lesquels apportent leur garantie financière permettant de garantir les risques – face auxquels les courtiers présentent les besoins des clients. 56 sociétés de gestions gèrent le syndicat dont sont membres des sociétés non britanniques d'assurance et de réassurance. Elles apportent leurs capacités pour avoir accès à ce système mondial. Le Lloyds est un marché de membres et n'est pas une société per se. Il est mentionné par un article spécifique du code français des assurances et de la réglementation européenne. Il constitue en lui-même un marché réglementé pour lequel s'appliquent les dispositions de l'autorité prudentielle britanniques PRA et des autorités des conduites financières britanniques FCA. La corporation des Lloyds dispose d'une autorité déléguée de la part du régulateur anglais pour contrôler elle-même son marché notamment dans le domaine de la quantification des risques et du suivi des cumuls.

- **Des capacités financières disponibles**

Les Lloyds sont présents dans 200 pays et territoires, représentent 36 milliards d'euros de prêts souscrits en 2016, dont 5% en provenance des Etats-Unis, 20% de l'Europe (Royaume-Uni compris). 68 milliards d'euros de sinistres ont été payés dans les cinq dernières années (pour illustration 4,2 milliards de dollars payés suite aux attentats de 2001, 20 milliards de dollars payés suite aux catastrophes naturelles de 2011). 258 courtiers agréés. 4.000 agents souscripteurs souscrivent pour les comptes du Lloyds de façon non exclusive, ils souscrivent pour plusieurs syndicats et disposent de plusieurs mandats. Le Lloyds est noté très positivement par les agences de notation ce qui constitue un élément clef de ce marché pour les clients cédantes et assurés. La qualité de la signature du Lloyds est déterminante pour la **chaîne de sécurité qu'il propose dont le premier maillon est de 63 milliards d'euros** – les actifs des syndicats mis en réserve mobilisables pour payer les sinistres. **Un second maillon d'une valeur de 25 milliards d'euros** de fonds est déposé par les membres. A l'intérieur du syndicat, les fonds déposés par une société les *Premium Trust Account* sont en vase clos. Un troisième maillon est constitué par les actifs centraux du Lloyds – **3 milliards d'euros de fonds de garantie du Lloyds disponibles pour payer la part de sinistre d'un membre insolvable**. Ces fonds ne sont pas placés sur le marché financier. **30% des fonds disponibles sont purement liquides**, 40% sont en emprunts obligataires et facilement liquides afin de pouvoir être en mesure de payer immédiatement le sinistre sans être dépendant des fluctuations du marché financier.

- **Face à une perception du risque hétérogène …**

Une étude des Lloyds[60] menée auprès de 40 dirigeants européens montre une réaction au risque cyber différente selon les pays. 52% des dirigeants français et allemands considèrent que les rançongiciels sont une troisième priorité alors qu'ils sont la première pour les Britanniques.

---

[58] Présentation Stratégie Cyber au Lloyds, par Guy-Antoine de la Rochefoucauld, Directeur général du Lloyds France SAS, mandataire du Lloyds en France.

[59] https://www.lloyds.com

[60] A report by Lloyds', « *Facing the Cyber Risk Challenge* », 20th September 2016, 22 pages.

42% seulement des entreprises s'inquiètent d'une potentielle fuite de données alors qu'ils ont été 72% à être victimes d'une attaque dans les cinq dernières années. Ce qui pose question en matière de méconnaissance du risque cyber et de sa gestion.

Concernant les dispositions du RGPD, 64 % des dirigeants craignent des enquêtes des autorités de régulation, 58% s'inquiètent des sanctions financières et 7% des clients interrogés connaissaient en 2017 à grands traits les dispositions du règlement européen.

- **… la réponse du Lloyds**

La question est comment apporter un service aux clients. Le marché apporte des réponses selon une segmentation de la typologie des clients entre les PME et PMI qui ont surtout besoin de services et les grandes entreprises qui ont essentiellement besoin de capacités. **40% des primes viennent des Etats-Unis depuis quinze ans suite à l'obligation légale de notification**.

Le premier poste assurantiel concerne le poste « organisation pour faire face le jour de l'incident », le second concerne « le coût potentiel pour l'assuré de l'attaque cyber ». Le programme d'assurance aide à faire face aux frais d'expertise informatique – selon le coût générique du nombre d'heures nécessaire ; une avance correspondant aux frais de communication de crise et de notification pour répondre aux enjeux de réputation (couverture de frais liés à un support d'experts qui va aider l'entreprise) ; ceux engendrés pour mettre fin à la tentative d'extorsion et de rançon ; les frais de reconstitution des données par exemple placées chez un prestataire de service indélicat payé). L'assistance vise d'abord la réduction du risque et des conséquences financières de l'attaque cyber. Le Lloyds assure également la perte de chiffre d'affaire, de marge brute et les frais inhérents au retour à l'activité ainsi que les frais de défense et les conséquences pécuniaires associées et enfin les frais d'enquêtes et les sanctions administratives (hors France).

Le Lloyds répond en partie à la perte de donnés et de biens immatériels notamment dans le cadre de la *business interruption* appliquée aux problématiques du cyber du client ainsi qu'aux conséquences de perte de marge brute si le fournisseur et le sous-traitant sont également victimes. Le risque digital intangible sur la réputation, la perte de propriété intellectuelle, de brevet et l'atteinte à la marque est adressé.

- **Ce que demande le Lloyds à ses clients**

Pour le Lloyds, la question n'est pas de savoir si le client va subir une attaque mais « quand ». Dans cette perspective, le Lloyds demande à ses clients d'identifier les risques spécifiques auxquels ils sont confrontés ; de s'informer sur la menace et l'évolution de la réglementation ; et de se former en continu. Il est attendu des courtiers qu'ils analysent les besoins des clients – sur le risque de réputation un dialogue doit être engagé avec le directeur financier.

- **La stratégie du Lloyds pour connaître et quantifier les risques sur son marché**

Le Lloyds définit ainsi le risque cyber : « un acte malveillant électronique qui provoque une perte dont les conséquences peuvent inclure des pertes de bien, de responsabilité, des atteintes aux personnes, des pertes financières ou toute autre sorte de dommage ». La réputation est inclue.

- **L'évolution des chiffres**

En termes de fréquence mondiale : plus 48% de 2013 à 2014 – 117300 attaques par jour. Le taux d'incident détecté depuis 2009 augmente année après année de 66%. La moyenne financière des pertes au niveau mondial entre 2013 et 2014 a augmenté de 34% soit 2,7 milliards de dollars.

Les primes souscrites proviennent à 80% du marché nord-américain, 6 % du marché britannique et 1% de l'Europe continentale. La progression : 2014 – 206 millions de Livres ; 2015 – 322 millions de Livres ; 2016 – 500 millions de Livres. L'entrée en vigueur du RGDP devrait faire évoluer les chiffres.

L'estimation du marché en 2016 était de l'ordre de 2,5 milliards de dollars (chiffres *Swiss-Re*). Ce dernier devrait atteindre en 18 milliards de dollars en 2025. Une branche cyber a été créée en 2013.

On perçoit une forme de spécialisation de la réponse par profil d'assuré potentiel dans le sens où chacun des syndicats a sa propre stratégie. Ex. *Beazley* développe des produits standards dédiés aux PME PMI – 1 ou 2 millions de chiffre d'affaire apportant du service. La tranche au-dessus montre un mix entre capacités et assistances. Le service est le même pour la grande entreprise mondialisée : les prestataires informatiques des Lloyds peuvent se déployer de par le monde en cas d'attaque.

- **Le contrôle et la surveillance opérés par le Lloyds pour être en mesure de payer le sinistre**

Dès 2015, avant que les autorités britanniques ne se saisissent du sujet, les Lloyds se sont engagés pour le contrôle et la surveillance de leur marché qui doit rester innovant. **Il est demandé aux syndicats d'identifier et de comprendre leurs risques lors de réunions pour écarter le risque de cumul potentiel** ainsi que les *silent cover cyber* dans leurs programmes traditionnels. Il leur est demandé de prouver qu'ils « savent » et de les quantifier de telle sorte à connaître le risque catastrophique y compris en *silent cover cyber*. **Les actions** pour atteindre ces trois objectifs sont une **demande concernant l'appétence au risque** – chaque syndicat doit informer et justifier des détails de la gestion des risques cyber, de **la compréhension de ce qu'ils souscrivent** et **de la prime demandée même en *silent cover cyber***. Le souscripteur doit connaître son portefeuille. Spécifier les « codes »[61] qui correspondent au cyber pour comptabiliser ensuite le nombre de couvertures identifiées comme telles pour pouvoir faire le montant du portefeuille. En ce qui concerne l'exposition au risque silencieux, l'approche est par scénarios catastrophe dont la liste a été agréée par la PRA. Chaque syndicat doit reporter ses engagements sur ces différents scénarios de stress test sur son portefeuille. C'est la vulnérabilité du porteur du risque (l'assureur) qui doit être mise au jour, le ou les évènements qui vont toucher de façon indifférenciée un volume suffisant d'assurés. Un *reporting* sur la base de leurs propres scénarios de crash test est exigé. C'est au syndicat de démonter ce qu'ils font, quoi et comment.

Le Lloyds a mis en place pour fin 2017 une évolution contrôlée des produits cyber du Lloyds, encouragé les clauses dédiées, mis en place des outils de quantification des cumuls, des bonnes pratiques et réduit le potentiel des *silent covers* cyber.

Le marché de l'assurance en France et au Royaume-Uni réfléchit à comment apporter des réponses aux besoins de couverture pour les biens intangibles par des couvertures dédiées ou intégrées même si des *wording* standards sont en cours en termes d'exclusion cyber.

---

61 les codes pour les branches spécifiques cyber ont déjà été créées, applicables depuis 2015 (CY depuis 2013): CY: Cyber security data and privacy breach: Coverage in respect of first or third party costs, expenses or damages due to a breach (or threatened breach) of cyber security and/or privacy of data, that does not include damage to physical property ; CZ: Cyber security property damage: Coverage in respect of first or third party costs, expenses or damages due to a breach of cyber security that includes damage to physical property Cyber policies where property damage is covered (physical property does not include loss of or damage to data in electronic form). Quand la couverture principale d'une police n'est pas le Cyber, les autres codes s'appliquent. Cependant, d'après les guidelines, dans le cas d'une large police globale (multirisques), une division des codes devrait être réalisée en fonction des expositions majeures et cette répartition appliquée à la prime de risque.

X.2. La réponse des Assurances et de la Réassurance sur l'assurabilité des intangibles

A la suite des présentations de ce qu'est un bien intangible et de ses possibles valorisations, la FFA et l'APREF se sont réunis par trois fois pour traiter ce sujet.

Si le sujet est bien évidement pertinent, en matière de risque cyber, il n'est pourtant pas perçu comme prioritaire tant par les assureurs que les réassureurs. En effet, avant de s'atteler à trouver des réponses sur l'assurabilité des intangibles, le marché de l'assurance doit, en premier lieu approfondir sa maîtrise du socle de l'assurance cyber – les définitions communes, les couvertures silencieuses, la maîtrise des engagements etc. Malgré cette priorisation, des pistes pour avancer sont déjà visibles et méritent d'être explorées ainsi qu'elles ont été évoquées lors des débats dans le cadre du séminaire de l'IRT.

X.2.a. La position de la FFA [62]

La réflexion du groupe de travail de la FFA sur le risque cyber est basée sur les fondamentaux suivants : l'assurance étant une activité réglementée et encadrée par l'ACPR, le code des assurances suit **un certain nombre de principes généraux** : notamment **le principe selon lequel l'objet du contrat d'assurance est de remettre l'assuré dans la situation dans laquelle il était avant le sinistre**.

Comment l'assurance peut-elle indemniser des biens intangibles ? De quoi parle-t-on ? De la perte des marchés futurs qui sont la valeur de bourse d'une société ? Des conséquences du vol des données et de leur valeur ? Pour apporter une première réponse deux principes sont énoncés ; **l'indemnisation vaut s'il existe une perte ou un préjudice qui soit certain (durable et mesurable).** Il s'agit d'**établir un lien de cause à effet entre la perte** – le préjudice, **le dommage** et **l'évènement** à l'origine et identifier la couverture afférente et ses conséquences.

- **Le cours de bourse**

Le préjudice certain et durable permet d'être un point de référence pour comparer les demandes faites. Concernant la valeur de bourse – le cas ***Target* : le chiffre de bourse a baissé de 25%** suite à l'attaque. **Deux ans plus tard le cours a dépassé la valeur qu'il avait à l'époque**. **Quel est donc le préjudice** subi par *Target*, plus précisément celui subi par ses actionnaires. Y a-t-il eu préjudice ? L'assureur peut-il intervenir ? Il est difficile d'apprécier la chute brutale du cours de bourse comme étant un vrai préjudice durable.

Peut-on faire une analogie entre la chute du cours de bourse avec une société qui, ayant subi un incendie, perd son chiffre d'affaire pendant trois mois ? Deux ans après, le CA est de retour mais ce dernier a bien subi une perte. Il s'agit de ne pas confondre le CA au titre de l'exercice n+1 qui est peut-être supérieur et le remboursement. L'indemnité est basée sur la perte d'exploitation et correspond bien au CA qu'il n'a pas réalisé pendant la période d'indemnité qui a suivi le sinistre. L'assureur **indemnise sur une période donnée** – sur une temporalité qui doit être déterminée. Dans ces conditions, comment indemniser une attaque cyber qui a eu un impact sur le capital social d'une entreprise, sa capacité à se financer, et dans l'ensemble sur tous les éléments qui ont trait à la richesse de l'organisation ?

En matière de **chute du cours de bourse, on est sur de la perte putative** – sur des effets induits sur la capacité de financement – ce qui n'a rien à voir avec le quantum de perte d'un actionnaire qui revend au pire moment

[62] Présentation par Philippe Gaillard, AXA, au titre de la présidence du GT cyber de la FFA.

du cours de bourse. Mais entre dire « il n'y a pas eu de perte » et « la perte n'est pas représentée par le cours de bourse », c'est autre chose. Qu'est-ce que la perte durable ?

Or, l'assurance n'est pas là pour assurer les pertes financières en bourse à différencier de l'indemnisation de la perte de l'entreprise sur sa perte d'exploitation. Faut-il dans ce cas dissocier et apprécier les conséquences ?

Comment donc lier une conséquence à un évènement qui est *triggé* et couvert par une police d'assurance ? On parle d'indemniser une perte sur la notion de la valorisation d'une chose à un instant donné. La valorisation du CA est un flux réalisé ou pas dans une période. On est matériellement sur des choses très différentes.

L'assurance rencontre des difficultés à apprécier les conséquences sur le cours de bourse après une attaque cyber. Si l'on ne tient pas compte des faits générateurs, mais seulement des pertes, la vraie question n'en demeure pas moins que **le lien de causalité est difficile à établir entre l'attaque cyber et la chute du cours de bourse**. **Derrière c'est la e-réputation** et **la confiance qui sont mises à mal**. Dans l'affaire *Vinci*, si on peut faire l'analogie avec une attaque cyber l'aller-retour du cours de bourse fut tellement rapide que l'assureur n'a même pas eu le temps d'être sollicité. Comment démonter le dispositif et démontrer une perte subie suite au mécanisme artificiel mis en place par malveillance pour acheter au plus bas des actions et vendre au plus haut ?

- **Vol de données confidentielles**

Deux impacts sont à considérer. **La perte du marché futur** qui peut être la conséquence du vol de cette donnée confidentielle et le **vol d'une marchandise** « la donnée » **avec la capacité des assureurs à mettre une valeur sur cette donnée.**

Or, aujourd'hui, **on ne sait pas mettre de valeur sur une donnée** car par nature la valeur pour une donnée n'est pas la même pour tout le monde et elle va dépendre de qui a intérêt à l'avoir pour en faire quoi. **Elle a donc un effet relatif**. **L'analogie avec le vol de marchandise qui a disparu n'est pas possible**. On peut parler d'« une copie ou d'un clonage». La connaissance liée à la donnée est restée à l'intérieur de l'entreprise. **Il faudrait arrêter de parler de vol de donnée et parler de perte de confidentialité, ou de privation réelle d'un capital intellectuel.**

L'impact sur les données personnelles, financières et de santé est plus facilement appréciable. Donner une valeur à ce dont a été privée l'entreprise n'est pas possible aujourd'hui.

Autre exemple lié à l'aspect RC. Quand les données ont été divulguées et qu'elles sont dans la nature, les personnes concernées peuvent craindre que leurs données aient été divulguées. **Comment calculer un préjudice en RC**. **Au tribunal, le juge est souverain pour décider**. Pour une personne, comment calculer le « préjudice psychologique » de savoir que ses données sont dans la nature et peuvent être potentiellement dévoilées. Les méthodes n'existent pas aujourd'hui pour calculer la perte et le préjudice pour pouvoir l'indemniser.

Prenons **le cas d'un laboratoire pharmaceutique** qui a investi des milliards dans le développement d'une molécule. Si la donnée est copiée par un concurrent qui lance un produit similaire sans avoir dépensé les mêmes montants de R&D et donc avec un prix plus attractif, **la perte est évidente**. Certes, mais dans ce cas le sujet pour l'assurance bascule sur l'espionnage économique. **Comment donc établir réellement le lien de cause à effet** ? Dans ce cas, comment être certain que la perte d'un marché est la conséquence de ce « vol » ou d'une copie de données.

Comment concilier le fait que lorsque la R&D investie est « perdue », il est clair que tout l'investissement est perdu. La perte est réelle. L'assurance ne couvre pas les dommages de risques opérationnels subis. On revient à l'hypothèse du risque pris par l'entreprise en fonction de sa stratégie business et l'assurance n'assure pas le risque d'entreprise au principe qu'il n'y a pas d'aléa.

Dans un monde idéal, l'investissement en R&D a été fait. Mais qu'est ce qui prouve qu'un autre concurrent n'était pas en train de progresser pour arriver quelques mois après sur le même marché ? Il n'est pas possible de dire, j'aurai forcément eu le marché, j'aurai forcément été libre de toute concurrence… **Il est quasiment impossible de démontrer à l'assureur la privation absolue d'un marché**.

Si l'on poursuit le raisonnement, l'autorisation de mise sur le marché d'un produit pharmaceutique suppose la réalisation d'un certain nombre d'essais cliniques. L'ensemble de ces essais sont produits de façon dématérialisée. L'atteinte à un de ces éléments dématérialisés fait que l'autorité qui délivre met en suspend l'autorisation. La molécule est là, elle est performante sauf que pour être mise sur le marché, les essais cliniques ont été compromis. Du fait de la disparition de ces éléments de preuve de la nocivité ou de l'innocuité, le laboratoire est contraint de refaire des essais cliniques. Deux ans de retard sur la mise sur le marché. Dans ce cas, des éléments économiques peuvent quantifier le préjudice. Le calcul du coût de deux années d'essais cliniques peut-être calculé, une couverture d'assurance spécifique pourrait être élaborée.

Est-il possible de calculer la perte de deux années de chiffre d'affaire en moins ? Non. On ne peut pas savoir de combien il aurait été. Quelle aurait été le taux de pénétration du marché. Peut-on au mois calculer l'amortissement, le retour sur investissement ? Pourquoi ne sait-on pas ? N'existe-t-il pas un contrat garantissant une vente future ? A-t-on besoin d'une garantie sur un contrat futur pour être indemnisé sur une perte d'exploitation en assurance ?

- **Le verrou est juridique**

Seulement pour la propriété intellectuelle, le législateur a mis la possibilité d'indemniser non pas les profits futurs mais les profits du contrefacteur en le condamnant. Au-delà de cette hypothèse-là, il est très difficile d'avoir une évaluation.

- **Le verrou est également comptable**

Il y a un vrai sujet sur la valeur de la donnée. Certes, cette question ne peut être rejetée car il en va de la créativité, de l'innovation des entreprises et de leur capacité à financer l'innovation dans la digitalisation. Si les assureurs déclarent ne pas reconnaître du tout cette nouvelle économie, il y a véritablement une situation de blocage.

X.2.b. L'intangible entre une approche traditionnelle et progressiste[63]

Dans une vision traditionnelle de l'assurance, le cyber ne doit pas conduire à réinventer le monde de l'assurance. Les règles du monde physique s'appliquent-elles au monde dématérialisé ? Quel est le changement de paradigme ? À la fin la relation est contractuelle, beaucoup de contrats couvrent des évènements qui sont aléatoires et cela marche très bien. Le contrat peut donc poser le risque cyber. A quel prix – prime ? Qu'est-ce que vous êtes capable de mettre en face – couverture. C'est une question d'*assesment* et d'analyse de souscription.

[63] Présentation de M. Sébastien Héon, SCOR.

- **Constat**

Les entreprises seront prêtes à payer le prix si les termes et les couvertures proposées sont valorisés par des référents. Mais indemniser sur la valeur des profits futur ouvre la porte à un contentieux sans fin sur comment on calcule, combien … **La question est comment rédige-t-on un contrat où le prix reflète la réalité du marché et qui soit juridiquement sécurisé**. Tout en respectant le principe de remettre l'assuré dans la situation dans laquelle il était (vision traditionnelle). Ce qui est aujourd'hui incomplet.

Deux traitements différents : les grands comptes face aux PME, TPE. Les grands comptes ont peut-être plus de facilités. Le sujet de la réputation est un sujet qui est lié à l'expression d'une perte mais pas seulement. Les PME ne déclarent pas qu'elles ont subi une attaque car elles ont aussi peur pour leur réputation. **Le sujet de la réputation est partagé** pour l'ensemble des entreprises et notamment pour une PME qui peut disparaître. Ce risque-là n'est pas actuellement adressé et les porteurs de risque sont seuls face à cette situation avec le risque d'une double peine.

L'assurance des pertes d'exploitation suite à question de réputation existe parfaitement dans d'autres pays et d'autres assureurs (UK les *Lloyds*) **avec le déclenchement d'un évènement garanti à la base**. L'agroalimentaire – *recall* d'image de marque est couvert par de tels contrats en France. La question appartient aux assurés et aux assureurs de savoir ce qu'ils souhaitent garantir. **Il s'agit de déterminer le déclencheur**, le niveau de garantie et sur le plan contractuel le prix. C'est un vrai sujet.

Pour autant le monde de l'assurance est conscient que ce n'est pas suffisant. C'est la raison pour laquelle, les contrats d'assurance cyber sont entourés de beaucoup plus de services que dans les contrats traditionnels pour accompagner le client à prendre des mesures d'urgence, à comprendre ce qu'il faut faire pour être conseillé, apporter des solutions, faire ce qu'il faut faire pour réduire au maximum le préjudice qui existe.

XI. Comment est-ce que la réassurance peut avancer sur l'assurance des biens intangibles.

Verrous

Retour sur la matrice des couvertures d'assurance cyber et sur la méthode SPICE qui permet au *Risk Manager* de maîtriser son exposition en quantifiant financièrement son risque cyber. SPICE n'a de sens que si le chiffre final est reconnu par les parties prenantes de la valorisation des données intangibles de l'organisation. Est-ce que ces règles peuvent être agréées par les différents acteurs ?

Après avoir entendu les membres du conseil d'administration et les professions en charge de la valorisation, la matrice développée lors des travaux de l'année 1 peut-elle être utilisée pour les biens intangibles ?

Pouvons-nous dès à présent associer à chaque cellule une norme et une formule pour développer la quantification ? Peut-on tester la matrice avec un auditeur ?

XI.1. Les réflexions pour la réassurance[64]

XI.1.a. Les chiffres du marché

Éléments chiffrés selon le *Swiss Re* Economic Reseach & Consulting, *Swiss Re Estimates* : le marché de l'assurance cyber existe aux Etats-Unis depuis vingt voire trente ans. Il s'établit autour de 2,5 milliards de dollars. **En comparaison, le cyber en Europe est loin derrière dans les autres lignes de business pour représenter 0,24 milliards de dollars en 2017**. Les polices dédiées (*Third Party, First Party, Extorsion*) en France sont estimées entre 50 et 60 millions d'euros. **Le montant maximum des capacités d'un programme cyber en termes de capacités proposé aux banques serait de l'ordre de 150 ou 200 millions d'euros**. **Entre 60 et 70% des entreprises du CAC 40 disposeraient d'une assurance cyber et toutes ont été approchées**. Les capacités disponibles sur le marché existent mais restent faibles. L'Asie se développe au regard de son niveau général d'assurabilité pour atteindre aujourd'hui 0,2 milliards de dollars de primes.

Ces chiffres doivent être lus en distinguant entre l'exposition et la couverture. L'exposition est en effet bien plus large que cela dans les montants en termes d'enjeux financiers. Une des questions qui se pose est de savoir si les chiffres présentés concernent des primes dédiées. Aucun chiffre n'est disponible en revanche sur la prime réelle sur l'ensemble des couvertures qu'elles soient dédiées ou intégrées à une police. Le pilotage de la prime est désormais plus ferme. Il est en effet demandé au souscripteur d'alerter sur son risque silencieux.

Le marché de l'assurance cyber est en croissance si l'on se réfère aux retours clients de *Swiss Re*. *Allianz* considérerait que le marché pourrait être estimé à vingt milliards de dollars à l'horizon 2025. Soit une croissance de primes additionnelles située entre 10 et 15% par an compte tenu de la dématérialisation des échanges.

XI.1.b. Les couvertures du cyber risque

Les couvertures dommages (*First Party*) portent sur les dommages subis par l'assuré : perte d'exploitation (BI, *Business Interruption*), les CIB (Contingent Business Interruption) qui couvre les carences des fournisseurs, les frais de restauration, les frais de notification et l'extorsion.

[64] Présentation de Patrick Richard, responsable du département Facultatives, RC *Swiss Re* – Paris.

Les couvertures responsabilité civile (*Third Party*) portent sur les dommages subis par des tiers lors du traitement ou la perte de leurs données permettant l'indemnisation des réclamations, et le paiement des frais de notification ainsi que les frais de défense.

Les extensions de couverture adressent les médias, lorsqu'une information « volée » à un tiers ou perdue va alimenter un réseau : la fraude, les pénalités adressées à un client quand il est prouvé que les moyens de sécurités mis en place n'ont pas été suffisants : les *credits cards monitoring*, les *PCI fines* demandés par les organismes bancaires.

Les exclusions « classiques » au sens de *Swiss Re*, au-delà des langages et des définitions variés qu'utilisent les courtiers et des différences qui existent entre les exclusions en Europe continentale, au Royaume-Uni et aux États-Unis, sont les suivantes – la guerre n'est pas garantie, ni la *Cyber War*. Les dommages corporels et matériels sont couverts par ailleurs. La propriété intellectuelle (*Intellectual Property*), le droit des marques (*Patent Infrigment*), les brevets, le secret des affaires (*Trade Secret Misappropriation*) sont difficiles à monitorer, modéliser et contractualiser. Il est en de même pour la réputation. Enfin les *Contractual Liabilities* : la prestation d'un client elle-même ne peut pas être couverte.

XI.1.c. Un paysage assurantiel changeant et diversifié

Il n'existe pas de standard sur la partie assurance cyber, mis à part le *German GDV model policy.* Au Royaume-Uni, le standard de police est « de péril dénommé ». En France, ce n'est pas toujours le cas.

L'environnement réglementaire évolue vite, notamment au niveau européen qui oblige de prendre en compte la protection des données.

Le marché se distingue par une grande variété de produits et de protections. Les produits américains couvrent la perte de données. En France, les garanties les plus recherchées sont des garanties de perte d'exploitation (PE) suite à une attaque. En Asie, la demande porte sur le cyber crime.

XI.1.d. Les limites de l'assurabilité

Les limites de l'assurabilité viennent des scenarios extrêmes tels que l'arrêt des communications qui est difficilement modélisable. Les couvertures silencieuses constituent un risque réel pour les traités de réassurance. **Les sociétés de réassurance souhaitent savoir ce qu'elles ont dans leurs bilans en face des positions prises par les assureurs ainsi que les réserves à mettre en regard à leurs expositions**. Les autorités de contrôle et les régulateurs se sont saisis de ce sujet au Royaume-Uni. La France devrait suivre.

Hors CAC 40, **les PME et les ETI** n'ont pas nécessairement les moyens d'acquérir une police dédiée fut ce à hauteur de dix milles euros. Quant aux TPE/PME, ont-elles conscience du risque cyber ? Mais **comme le risque cyber n'est pas exclu, ces polices (RC, incendie) peuvent être appelées au titre d'un sinistre cyber. Dans ce cas, les polices ne sont pas adaptées. Ainsi, la PE non consécutive à un dommage matériel pourrait, par exemple, être couverte. On se retrouve alors avec des risques immatériels qui sont consécutifs à des risques non garantis qui couvrent en partie du cyber**.

Un consensus existe sur le fait que l'absence de souscription par les entreprises de contrat cyber mais, également, la non connaissance de l'articulation des garanties RC, de Dommage et de Cyber pur ne dresse pas un environnement clair en cas de survenance d'incident cyber d'importance.

Or aujourd'hui, le constat est le suivant, **il n'y a pas de sinistre**. Ainsi le travail mené par l'IRT-SystemX doit permettre une prise de conscience afin d'éviter d'importants problèmes économiques en cas de survenance d'un évènement cyber d'une grande ampleur.

Le réassureur dispose de quelques méthodes pour calculer ses cumuls. Il mesure l'exposition – les risques engrangés et monitorés par rapport à du *benchmarking* de secteurs industriels, des éléments géographiques, par types de police RC. Le second élément est l'expérience : quel est l'historique des évènements, comment se rattacher à de l'existant ? Ensuite, la diversification. Dans une vision « traité », le prix est affecté à un portefeuille. Pour le cyber, cette méthode est compliquée à appliquer parce que l'historique fait défaut. Que vaut le risque cyber d'une société d'électricité par rapport à celui d'une entreprise de manufacture classique ? Il y a aujourd'hui quelques affaires mais peu d'éléments comparatifs. Il y a des experts mais peu de matière à partager. La difficulté aujourd'hui est le phénomène d'accumulation dans les traités pour lesquelles les méthodes d'appréciation sont empiriques. Certaines compagnies de réassurance utilisent les modèles CAT pour calculer les SMP. La position de *Swiss Re* est de rester sur des hypothèses plausibles à partir d'observations de listes de portefeuilles. Actuellement, *Swiss Re* réutilise peu de modèles ayant fonctionné dans d'autres branches d'assurance.

- **Quatre cas répertoriés**

La rupture de service (DOS) et l'interruption d'opération (IO) – les hypothèses d'attaque sur un portail commercial, sur un serveur cloud ? Ces évènements devraient être garantis par des polices spécifiques. La rupture de service est le scénario le plus souvent envisagé pour le marché français. Il fait l'objet d'une demande importante. La difficulté de ce scénario réside dans le fait que la perte d'exploitation pourrait être consécutive de deux évènements différents pouvant s'accumuler.

Le scénario cloud est également inquiétant face à la multiplication des services opérés, leur absence de transparence, le manque de réglementation les concernant et le fait que leur défaillance peut avoir un impact mondial. La résilience de l'infrastructure Internet et ses impacts mondiaux pose interrogation. Un même incident peut avoir des répercussions au niveau mondial touchant une multitude d'assurés et d'assureurs.

L'Amazon Web Service du 1er mars 2017 a connu des dysfonctionnements. L'évènement a bloqué l'accès internet aux clients de la plateforme pendant quelques heures. Cet évènement peut-il être compris comme un scénario d'accumulation du point de vue du réassureur ? A la connaissance de *Swiss Re*, aucun sinistre n'a été remonté. C'est tout le problème de la matière cyber.

Les *datas breaches* ou **le vol de données** (personnelles ou bancaires) – ces derniers devraient faire l'objet d'une couverture dans des polices spécifiques.

Les infrastructures critiques (avec ou sans dommage matériel) font l'objet de garanties dans des contrats classiques tout comme le *failure to supply* avec des conséquences en responsabilité civile qui peuvent être garanties également par des polices classiques.

- **Les scénarios de cumul par industrie**

Le secteur financier et assurantiel fait l'objet d'une attention forte à cause de la volatilité des marchés et de l'intensité des impacts financiers subséquents. Viennent ensuite le e-commerce, puis les infrastructures critiques et la santé.

L'ensemble des traités dans lesquels il y aurait des couvertures immatérielles relatives au digital est répertorié. Un effort de calcul du montant des primes est conduit par rapport aux déclarations des lignes bussiness (*layers*) produit par les assurances. Les méthodes et les modèles sont assez empiriques et évoluent dans un souci d'amélioration constante.

Une solution serait de partager davantage avec les clients – les assureurs et que ces derniers échangent plus avec leurs assurés et les industries afin d'obtenir un maximum d'information pour affiner l'analyse. Les challenges sont la compréhension et le suivi de l'évolution des techniques d'attaque, la quantification du risque cyber, une évolution des réglementations, une modification constante des modèles, espérer que des sinistres soient enfin déclarés et surtout que les couvertures silencieuses soient insérées dans les traités soient identifiées.

XI.2. Position de l'APREF[65] – comité système d'information : les potentielles difficultés au développement du marché de la cyber assurance

XI.2.a. Où se situent les spécificités de l'assurance cyber ?

L'assurance cyber est-elle unique ou pas ? Si l'on regarde dans le détail, beaucoup de choses existaient déjà et sont aujourd'hui appliquées au cyber lorsque les mécanismes sont assez proches. Les couvertures cyber extorsion ressemblent aux *kidnapper ransom* dans leurs mécanismes et leur façon de fonctionner. **De nombreuses couvertures cyber ont leur équivalent des garanties standards qui existent depuis longtemps** – tout ce qui est notification de perte de données et de gestion d'incident ressemble aux garanties « rappel de produit ». La fraude qu'elle soit faite à l'aide d'un SI ou en utilisant un ordinateur reste de la fraude. La perte d'exploitation reste de la PE quand un système d'exploitation s'arrête ou que l'usine est en panne. Le péril cyber ne fait que générer de nouveaux challenges et poser de nouvelles questions.

Une des questions majeures reste l'assurabilité des biens intangibles. Restée en suspens, cette interrogation demeure une question ouverte. Le cyber ouvre de nouveaux besoins mais peut s'inspirer de l'existant de certaines couvertures. Si l'on compare le schéma d'une chaîne d'approvisionnement et celui d'un système d'information, ces objets recèlent des similitudes et si l'on arrive à travailler la question des CBI en profondeur, peut-être que certains éléments pourront s'appliquer au cyber.

Des sujets connexes peuvent faire l'objet de comparaisons utiles à la réflexion.

Le marché de l'assurance cyber ne doit pas être présenté au sens large car il se décline en éléments très différents – des produits *stand alone* explicitement cyber, des amendements ou des extensions à des contrats standards et puis des produits bicéphales avec des garanties D&O, RC pro et des garanties cyber entremêlées. **Il existe toute une typologie de produits qu'il s'agit de distinguer**. Ce n'est pas en réalité une situation satisfaisante pour la connaissance des expositions mais le marché manque encore de maturité… ce qui est en soit un frein à son développement.

Des défis – la prise de conscience des impacts potentiels. Quelques cas concrets éclairent sur des situations qui n'étaient pas forcément intuitives. Par exemple, une campagne de cyber attaques massives telles que *WannaCry* ou *NotPetya* n'ont pas pour conséquence essentiellement des pertes des données mais dans de fortes proportions des pertes d'exploitation et d'interruption de service. Ces deux évènements ont fait l'objet de remontée à chaud par certains *risk managers* dans des cercles restreints (AMRAE). Le *Risk Manager* de *Renault* et le RSSI par exemple ont fait un retour d'expérience sur leur gestion de la crise post *WannaCry*. L'ANSSI de son côté communique avec l'assentiment de la victime.

Les chiffres du *Lloyds* montrent l'ampleur du risque cyber avec une composante systémique du risque cyber sur l'inter-connectivité de plus en plus large. Un point de préoccupation – les différents stress tests que l'on voit se dessiner attaque après attaque tel le blackout sur l'Ukraine, l'attaque sur *Swift*, les impacts de *WannaCry* et *NotPetya* sur les infrastructures critiques.

- **L'importance de scénarios réalistes**

Dans quelle mesure peut-on taxer ces présentations comme étant un des outils marketing utilisé par les assureurs pour augmenter les ventes par des arguments de peur ? Il est aujourd'hui constaté un très faible retour sur les sinistres quantifiés dans le domaine cyber alors que le marché répond très bien aux demandes climatiques estimées en milliards

[65] Association des professionnels de la réassurance déployés en France. Présentation préparée par la Commission Cyber de l'APREF.

de dollars. **Qu'est ce qui donne aujourd'hui de la crédibilité à ce genre d'annonce par rapport au fait que le retex de l'impact du sinistre est faible ?**

Premier point : **dans le domaine cyber, il n'y a pas encore eu d'évènement catastrophique de grande ampleur**. **A contrario dans la sphère individuelle, les impacts économiques sont énormes**. Le coût de l'attaque cyber de *Target* est évalué à 300 millions de dollars, plus le coût des *data breach*, de la notification, de la réémission des cartes *American Express* des clients, trente-quatre millions de dollars d'amendes. Dans l'absolu cela peut être considéré comme relatif mais à titre individuel, les montants sont très élevés pour les organisations. L'acteur économique risque sa survie sur un seul risque et le niveau de prime reste très bas et sans analyse car il n'existe pas encore de référence financière sur le coût de l'impact économique du risque cyber. Voir les travaux sur ce sujet entrepris par l'OCDE SPADE.

Dans le domaine de l'aéronautique la problématique est complètement différente. L'équation prime, fréquence et volume conduit à ce qu'il n'existe pas encore de prime pour faire face au risque cyber.

Second point : les scénarios pour modéliser les conséquences d'une catastrophe de grande ampleur. Il pourrait être intéressant de partager les scénarios PIRANET de l'ANSSI[66] par exemple pour savoir si des scénarios d'ampleur au niveau national France pourraient survenir.

Une tendance lourde se dessine dans les grands comptes. Dix ans auparavant, les connexions des acteurs économiques passaient par les acteurs des télécoms. La sensibilité à la rupture d'interconnexion était limitée. Les connexions ont depuis migré vers des lignes VPN supportées par internet pour la majorité des connexions entre différents sites, clients, partenaires et fournisseurs. Ce mouvement s'est accompagné d'une sous-estimation du risque d'exposition des entreprises. **La remise en service ne passe plus par l'opérateur télécoms**. Vers qui se tourner si l'internet tombe ? Et si plusieurs grands acteurs utilisent les mêmes infrastructures, le risque se cumule. Cette évolution fut silencieuse.

Or, la difficulté pour mesurer le caractère systémique ou non ou « transverse » vint du fait que les scénarios publiés sont extrêmes notamment aux Etats-Unis – plus d'électricité, la population s'entretue ; dès lors le vecteur cyber devient relatif. De l'autre côté, des scénarios sont présentés par des personnes qui pensent que, finalement, le risque cyber c'est beaucoup plus de bruit pour pas grand-chose quand on regarde l'historique des attaques et des sinistres.

La vérité est sans doute au milieu et toute la difficulté est d'obtenir un scénario crédible validé par des professionnels. Il faut que le scénario soit connecté à la réalité et réponde aux plans de secours, aux enjeux de crise auxquels font face les acteurs. Les scénarios doivent tester la capacité des acteurs à gérer le risque cyber et à réagir en temps et en heure. Un scénario basé sur une histoire réaliste permettrait d'identifier les différents acteurs de la chaine et de comprendre les réactions des parties prenantes dans un volant d'heures limité. **On dispose de peu d'éléments objectifs pour identifier la part du digital dans l'économie et en miroir nous disposons d'aussi peu d'éléments objectifs pour mesurer l'impact économique du risque cyber**. Il s'agit de se poser la question de savoir **quels pourraient être les éléments qui pourraient crédibiliser ces analyses de façon rationnelle**. Nous constatons le passage entre une ancienne économie et une nouvelle basée sur le numérique et sommes encore dans une période de transition qui ne permet pas encore une communication simple sur les risques et leur fréquence. La multiplication des évènements et l'éducation feront évoluer les pratiques. Le rythme est lent au regard des enjeux.

XI.2.b. Le cumul du risque n'est pas maîtrisé

Si les réassureurs s'estiment crédibles dans leurs analyses des branches traditionnelles, est-ce que les méthodes de réserve interne sont adaptables au risque cyber qui existe dans les portefeuilles ?

[66] Les exercices PIRANET relèvent du secret de la défense nationale. Leur objectif est d'obtenir un scénario relativement crédible afin de valider un plan de réaction. Ils s'inspirent de la réalité. Leur but n'est pas de tester les effets systémiques d'une attaque.

Les modèles sur le connu sont robustes mais les réassureurs ont du mal à modéliser ce qu'ils ne connaissent pas. Ils adoptent donc une posture conservatrice mais travaillent sur ces questions. L'ensemble des contrats sont relus pour identifier les *silent covers*, les contrats dédiés etc. Le *risk management* en interne assurance s'est saisi de ce sujet. Meilleure sera la connaissance de ces sujets, plus facile sera la réassurance.

- **Les freins**

Du côté de la demande, les primes sont jugées élevées. Les protections sont perçues comme inadéquates ne couvrant pas ce qu'il faudrait. L'évaluation des besoins de couverture reste difficile. Associer un coût face à un scénario cyber reste compliqué. Des études sont menées, des méthodes commencent à apparaître mais elles ne sont pas encore assez répandues. Du côté de l'offre, certains réassureurs considèrent que le marché de l'assurance cyber est une bonne opportunité de croissance. D'autres demeurent prudents. La diversité du marché est intéressante face à une exposition qui demeure complexe dans un marché jeune et pas encore stabilisé. Les fondements sont en cours d'installation, le périmètre est encore flou. L'assurabilité des biens intangibles pose problème.

- **Besoin de capacité et allocation du capital**

Par rapport à la capacité offerte par la réassurance, quelle est l'allocation du capital pour permettre de couvrir la capacité proposée ? Comment sécuriser le ratio de solvabilité ? Ce point explique en partie que le démarrage du marché est assez lent et prudent. Le marché de la réassurance est estimé à 500 millions de dollars de primes de réassurance face aux 3 ou 4 milliards de primes d'assurance cyber. Principalement des traités.

Certains assureurs souscrivent en net sur des risques PME, TPE, ou individuels. Dès lors que de gros risques sont adressés, la réassurance est impliquée. Au regard du faible nombre de couvertures d'assurance souscrites, le sujet de la capacité n'est pas encore prégnant. Ainsi aujourd'hui, le marché cyber est plus un marché (américain) de l'assurance que de la réassurance. Le cumul existe donc en premier lieu dans le bilan des compagnies d'assurance. Dans la mesure où ils souscrivent des affaires, c'est à eux d'identifier le niveau d'exposition qu'ils sont prêts à conserver mais cette analyse s'avère relativement difficile à conduire. Certains acteurs s'interrogent en effet, sur le fait de savoir s'ils ont trop souscrit et s'ils vont pouvoir faire face en cas de sinistre global et systémique. La réassurance leur permet de céder une partie du risque et de protéger leur bilan selon plusieurs mécanismes possibles : facultatives, traités non proportionnels (excédent de sinistres ou *stop loss*) ou proportionnel.

Quand un assureur offre une garantie à 150.000 euros, il n'a pas besoin de réassurance. En revanche, s'il en souscrit plusieurs (50.000, 100.000 ou 1 million etc.), il réfléchit à l'occurrence d'un évènement catastrophique. L'assureur peut conserver une partie de ce risque « évènement » (une part acceptable au regard de son bilan) et en céder l'excédent, au-delà d'un seuil contractuellement déterminé au réassureur, en échange d'une prime cédée. C'est la raison pour laquelle, sur cette masse de petites mises souscrites, la prime de réassurance pourra être faible. Le réassureur n'interviendra que lorsque l'assureur sera en limite. Pour d'autres typologies de risques où des capacités plus grandes sont allouées ou quand l'assureur veut partager la masse de petits risques (pour limiter son exposition et/ou souscrire davantage), le réassureur intervient en quote-part. Dans ce cas-là, la prime est « partagée » avec l'assureur en fonction du taux de cession (plus ou moins élevé) – phénomène de co-assurance. Les 500 millions de primes proviennent à 95% de quote-part.

Comment comprendre la répartition entre 4 milliards de dollars de primes d'assurance et les 500 millions de prime de réassurance ? Est-ce un marqueur de prudence de la part des réassureurs ? Est-ce une volonté des assureurs de conserver la majeure partie de leurs risques qui génèrent pour l'instant de très bons résultats ou uniquement la résultante des types de réassurance utilisée ? Ce chiffre est révélateur d'une pratique de marché américain beaucoup plus mature et développée : plus de contrats mais de petits niveaux car correspondant aux impératifs de la réglementation qui protège les données personnelles et donc des risques conservés en grande partie par les assureurs. Des *primary cyber* de 5 millions de dollars de couverture sont assez généralisés. En France, quand on achète du cyber

c'est de l'ordre de 10 ou 15 millions d'euros en ticket de départ de couverture. Seules les affaires de grande importance bénéficient de réassurance – hors TPE/PME qui sont bien en deçà de ce seuil (cf. la police GAN).

Une PME fait 20 millions de chiffre d'affaires disposant d'une couverture cyber à hauteur de 300.000 euros ne mettra pas en péril son assureur mais si ces 300.000 euros sont multipliés horizontalement sur 10.000 polices, ils provoquent un effet d'accumulation. L'assurance et son réassureur quote-part, ou son réassureur CAT, vont alors devoir faire face à un sinistre de grande ampleur qui peut être d'autant plus grand chez le réassureur qu'il peut toucher plusieurs de ses clients assureurs (cf. gestion des cumuls) et ce, sans compter les expositions dites silencieuses qui peuvent en plus l'impacter.

Sur le cyber, du fait de ces accumulations, les réassureurs sont plus exposés que les cédantes. Aux États-Unis, une des forces du marché est qu'il existe une meilleure connaissance des profils de risque. En France, les besoins sont concentrés sur ceux qui ont beaucoup à perdre, sur une famille de risques très exposée. Ce qui pourrait modifier la donne serait l'obligation de notification des incidents comme aux États-Unis. Le coût de notification sur les *data breach* est extrêmement mécanique : obligation de déclaration, de traitement, de notification = le coût est connu. L'important est la capacité qu'a une organisation d'anticiper une perte financière.

XI.2.c. Fluidifier pour améliorer le marché

Chacun des acteurs a des questions à se poser pour fluidifier ce marché et assurer une meilleure assiette et stabilité au marché.

Les **risk managers** doivent améliorer la connaissance de l'exposition, des scénarios, de la stratégie de réduction des risques et de transfert. Faire en sorte que le risk manager dispose des bonnes cartes pour prendre les bonnes décisions.

Les assureurs devraient se pencher sur la sélection des risques : la qualité des couvertures et des exclusions ; la manière dont elles répondent ; les *silent covers* ; la question de la tarification. Le marché est actuellement « *soft* », compétitif sur les garanties traditionnelles comme sur le risque cyber. Il serait souhaitable que le marché satisfasse la demande sans sacrifier à des extensions de couverture données gratuitement, élargir les couvertures, réduire les exclusions et ce pour un montant de primes stable d'un renouvellement à l'autre du de la pression du marché.

Au niveau des réassureurs, les challenges sont le problème de la quantification et de la qualification des problématiques d'agrégation avec là encore, un besoin d'amélioration de la certitude dans la manière dont les contrats répondent. Le problème des *silent covers* dans les traités de réassurance et les produits sous-jacents.

- **Mesurer le poids de la réassurance dans le développement de l'assurance cyber**

Aujourd'hui, la réassurance n'est pas moteur dans le déploiement de l'offre d'assurance cyber puisque la plupart des assureurs souscrivent avec une rétention forte. La réassurance est également en seconde ligne après celle des assureurs. Quelle est la capacité de la réassurance pour être un véritable catalyseur du marché ?

Chacun des acteurs doit faire sa part. Les assurés doivent avoir une meilleure vision de leurs besoins de couverture et de capacité. Les assureurs doivent développer des produits qui correspondent à la demande tout en ayant un prix bien identifié et qu'ils se soient débarrassés des couvertures silencieuses, que la prime qui est attachée à la couverture du contrat soit identifiée. Les réassureurs doivent travailler sur le contrôle du cumul des agrégations et de scénarios permettant d'identifier l'exposition globale pour savoir si le changement en capital est suffisant ou pas.

- **Les marqueurs de l'évolution du marché**

Deux options, soit les réassureurs vont être en mesure de proposer au marché une plus grande capacité de réassurance pour permettre aux assureurs de déployer de nouvelles offres, soit ce seront les assureurs qui seront au contact des *risk managers* pour développer leur offre.

Le marché reste drivé par la demande. Or, elle est encore très faible en France et en Europe. Les acteurs ont de plus en plus conscience du « besoin » **mais entre le dire et exprimer un souhait**, la route est longue. Il y a également **un vrai sujet de la prime**. Les assureurs doivent exprimer une demande pour que les assureurs bâtissent une proposition. L'inverse semble compliqué. **Il semblerait que les assureurs aient des difficultés à répondre aux attentes des *risk managers* qui ne maîtrisent pas encore leurs expositions**. Les assureurs ne disposent pas non plus de réseaux de distribution nécessaires pour vendre de l'assurance cyber. **Le courtier a également du mal à aborder la question pour les PME ainsi que pour des entreprises plus importantes**. Le marché est encore attentiste. La prise de conscience est progressive.

On constate une augmentation de la demande de tarification mais les budgets des PME et ETI ne suivent pas pour payer la prime. Dualité entre la prise de conscience et l'inscription au budget d'une prime de 3.000 ou 4.000 euros. Enfin, plus les sinistres auront de résonnance plus la prise de conscience augmentera.

XI.2.d. Les pistes, les travaux des réassureurs

Plusieurs voies sont explorées.

- **Maîtriser les couvertures de réassurance**

Leurs étendues et leur tarification : la quote-part proportionnelle a ceci de facile qu'elle simplifie la tarification pour le réassureur. Tarifer du non proportionnel en cyber est compliqué. Revoir les clauses d'exclusions et le *wording* qui sont dépassés.

- **Définir un évènement cyber de type catastrophe**

Pour l'application des traités et des clauses de réassurance, comment définit-on un évènement de type catastrophe ? **Comment qualifie-t-on les incidents et les évènements, quels sont les critères ?** À la différence des autres sinistres catastrophiques, on ne peut pas proposer une même cause, une même origine, un même évènement, une clause horaire. Avoir une discussion sur le fait de savoir si *WannaCry* ou *NotPetya* sont ou non un même évènement au sens cyber n'est pas simple. Est-ce que si l'on avait un traité non proportionnel, seraient-ils considérés comme deux évènements différents ou un seul ? **La question de la définition est essentiellement une question pour la réassurance**. Sa résolution permettra de développer le marché et facilitera la vie des assureurs également.

Il faudra trouver une façon de définir un évènement qui soit compréhensible et partageable par tout le monde. **Cumul et évènements sont liés**. **Faut-il revenir sur les recommandations issues du rapport de recherche de 2016 ? Il s'agit de créer les définitions**. Celles qui sont négociées entre assureurs et réassureurs contractuellement créent de l'instabilité juridique. Pour le CAT, l'APREF a fait des propositions sur la cause commune et sur l'origine commune. Cela reste à faire pour le cyber – la cause commune étant difficile à définir, faut-il partir de l'évènement ?

Des solutions sur des clauses évènements ont été trouvées pour des éléments immatériels. C'est à la cédante d'exprimer par rapport à son portefeuille quel est son besoin. *AXA* n'ayant pas les mêmes besoins que la *Mutuelle de Poitiers* – leurs problèmes d'accumulation et d'impacts sur les bilans sont complètement différents.

- **Gestion des cumuls**

La question de l'agrégation est communément adressée mais le fait qu'il y a d'autres cumuls – le prestataire de services opérés peut interrompre son service, mais **il faut considérer également les clashs de polices** d'un même assuré qui répondent à un programme cyber, dommage, extensions au programme RC, D&O déclenchée par un évènement cyber. Il peut y avoir **plusieurs assurés qui peuvent être liés par la *supply chain* ou par des prestataires IT**. Ce cas est identifiable Ce qui est plus difficile à identifier est **le cas de plusieurs assurés qui subissent une attaque a priori non ciblée et qui sont victimes ensemble au même moment d'un même incident – plusieurs assurés de plusieurs assureurs et donc une accumulation de plusieurs traités**. On peut avoir **un assuré « grands risques » qui apparaît dans plusieurs traités différents** – coassurance : ce qui génère un problème de cumul pour identifier le ou les traités.

Et on peut avoir **plusieurs traités sur des lignes différentes qui eux même répondraient à un même incident cyber**. Une complexité de cumul par assuré. Plusieurs traités qui contiennent le même assuré qui peut avoir plusieurs polices qui répondent. Un enchevêtrement de cumuls difficiles à démêler. Certains éléments vont être payés plusieurs fois.

Un vrai problème compliqué si l'on rajoute la question des **silent covers et l'insécurité juridique**. L'identification nécessite une approche catégorisée et scientifique. Cette identification se fait sur d'autres lignes de business mais le manque d'antériorité sur le cyber est un frein.

Contribuer au développement du marché pour qu'il se structure et soit profitable sur le long terme. Créer la confiance est essentiel, une des possibilités serait de s'orienter vers des produits *stand alone* cyber cadré, identifiés avec des lignes définies, des franchises claires, savoir comment cela répond avec des primes correspondant et bien tarifées.

Organiser un exercice avec des objectifs – tester la robustesse des exclusions, pour des couvertures silencieuses la mesure d'impact pour l'assureur. Un scénario obéissant à des contraintes et une réalité – un degré de finesse pour que le scénario soit représentatif. Outillé. S'appuyant sur des cas réels. Apporter du sens en calibrant le scénario. Le partager avec une communauté ayant du poids.

Annexe 1 – La notion d'incident de sécurité à travers les normes et les textes réglementaires

Rédacteur : Jean-Laurent Santoni.

Les obligations de notification des incidents de sécurité aux autorités de régulation (CNIL, ANSSI, agences régionales de santé) prévues par des textes nationaux ou européens s'inscrivent dans un processus plus global de gestion de la sécurité. Toute entité informatisée doit se préparer à répondre à cette situation et le processus de gestion des incidents doit être pensé, testé, évalué et corrigé. Les obligations de notification aux autorités compétentes entrent pleinement dans le périmètre de ce processus, qui devient de facto un élément clé de l'organisation de tout organisme. En se basant sur les différents textes précités et en s'inspirant du processus de gestion des incidents défini par la norme ISO/IEC 27035, il est envisageable de prévoir, en interne pour chaque organisme, un processus propre de gestion des incidents. L'organisation doit ainsi être pensée en amont de l'incident et non pas lorsque celui-ci se produit. Une organisation efficace permet d'améliorer la gestion des incidents et de se conformer aux textes. Avant de s'intéresser à la notion d'incident de sécurité, il faut tout d'abord étudier ce qu'est un « événement de sécurité ». Or, les normes ISO 27001 (« Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information – Exigences ») et ISO 27002 (« Code de bonnes pratiques pour la gestion de la sécurité de l'information ») définissent la notion comme « **une occurrence identifiée d'un état d'un système, d'un service ou d'un réseau indiquant (une faille pour l'ISO 27001 ou une brèche pour l'ISO 27002J possible dans la politique de sécurité de l'information ou un échec des moyens de protection, ou encore une situation inconnue jusqu'alors et pouvant relever de la sécurité** ». Une fois que l'événement de sécurité survient, celui-ci peut, dans un second temps et en fonction des éléments de contexte applicables, être qualifié d'« incident de sécurité ». Cela dépend en pratique s'il tend à révéler une probable compromission des activités de l'organisme ou de la sécurité de l'information. Ainsi, les normes ISO 27001 et 27002 déjà mentionnées caractérisent la notion d'incident de sécurité « **par un ou plusieurs évènements intéressant la sécurité de l'information indésirable(s) ou inattendue(s) présentant une probabilité forte de compromettre les opérations liées à l'activité de l'organisme et de menacer la sécurité de l'information** ».

En fonction du domaine concerné, les textes réglementaires ont recours à un vocabulaire différent pour désigner cet « incident » qui a fait l'objet de plusieurs définitions distinctes, notamment en fonction du domaine concerné.

1. En matière de données à caractère personnel, où il est question de « violation de données à caractère personnel », les textes européens et français ont donné plusieurs définitions relativement proches des normes ISO. Ainsi, s'agissant de l'obligation de notification à la CNIL et aux personnes concernées imposée aux fournisseurs de services de communications électroniques accessibles au public, la violation de données à caractère personnel a été définie comme « une violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés de données à caractère personnel » faisant l'objet d'un traitement. Le règlement européen qui étend cette obligation à tous les secteurs d'activité, a toutefois retenu une définition qui ne mentionne plus l'incident de sécurité en lui-même et se concentre sur ses conséquences (« la destruction, la perte, l'altération, la divulgation ou la consultation non autorisées, de manière accidentelle ou illicite, de données à caractère personnel transmises, conservées ou traitées d'une autre manière »). Par ailleurs, le considérant 8 (qui n'est pas d'application directe en tant que tel, mais qui sert à interpréter les règles posées) du règlement n° 611/2013 du 24 juin 2013, qui vise à uniformiser le cadre de la notification pour les fournisseurs de services de communications électroniques accessibles au public, précise que : « le fait de simplement soupçonner qu'une violation de données à caractère personnel s'est produite ou de simplement constater un incident sans disposer d'informations suffisantes, malgré tous les efforts déployés à cette fin par un fournisseur, ne permet pas de considérer qu'une telle violation a été constatée aux fins du présent règlement ».

2. En matière de notification des incidents réseaux, l'article 13 bis de la directive 2002/21/CE modifié définit en réalité l'incident de sécurité au travers de ses conséquences. Ainsi, il y a un incident lorsque les « entreprises fournissant des réseaux de communications publics ou des services de communications électroniques accessibles au public » constatent une « atteinte à la sécurité ou perte d'intégrité ayant eu un impact significatif sur le fonctionnement des réseaux ou des services ». La transposition en droit français de ce texte a repris ces termes à l'identique.

Des termes également identiques sont repris dans la directive SRI (sécurité des réseaux et de l'information) publiée le 7 février 2013 qui étend cette obligation à un certain nombre d'acteurs économiques et définit l'incident comme : « tout événement ayant une incidence négative réelle sur la sécurité ». Cet « incident qui a un impact significatif » est lui-même défini dans le texte comme « un incident qui porte atteinte à la sécurité et à la continuité d'un réseau ou d'un système d'information et qui entraîne une perturbation notable de fonctions économiques ou sociétales essentielles ».

3. Le principe de cette obligation se retrouve à l'article 22 de la loi n° 2013-1168 « relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale » du 18 décembre 2013 qui intègre un article L.1332-6-2 au Code de la défense qui prévoit à la charge des Opérateurs d'importance vitale et « des opérateurs publics ou privés qui participent à ces systèmes » l'obligation de respecter à leurs frais des règles de sécurité particulières, mais surtout l'obligation de notifier sans délai au Premier ministre « des incidents affectant le fonctionnement ou la sécurité » de leurs SI. La formulation est ici beaucoup plus large.
4. Les prestataires de « services de confiance » (PSC) sont également concernés. Ainsi, le règlement européen sur l'identification électronique et les services de confiance du 4 juin 2012 (dit « elDAS ») dans sa version définitivement adoptée le 23 juillet 2014 les définit comme « une personne physique ou morale qui fournit un ou plusieurs services de confiance (...) » à savoir « un service électronique normalement fourni contre rémunération qui consiste en : a) la création, la vérification et la validation de signatures électroniques, de cachets électroniques ou d'horodatages électroniques, de services d'envois recommandés électroniques et des certificats relatifs à ces services ou b) la création, la vérification et la validation de certificats pour l'authentification de sites Web ou c) la conservation de signatures, de cachets électroniques ou des certificats relatifs à ces services » (article 3).

Ces prestataires de service de confiance sont ainsi tenus à une obligation de notifier « toute atteinte à la sécurité ou toute perte d'intégrité ayant une incidence importante sur le service de confiance fourni ou sur les données à caractère personnel qui y sont liées », auprès « de l'organe de contrôle et, le cas échéant », auprès de l'ANSSI ou de la CNIL. La notification devra également être effectuée auprès des personnes physiques ou morales auxquelles le service de confiance a été fourni lorsque l'atteinte à la sécurité ou la perte d'intégrité est susceptible de leur porter préjudice, ainsi qu'à l'ENISA voire au public lorsqu'il est d'utilité publique de divulguer cette atteinte.

5. En complément de l'encadrement rappelé ci-dessus, le législateur européen prévoit d'étendre le principe de notification des incidents de sécurité à d'autres secteurs économiques. Dans le domaine d'étude qui nous intéresse ici, retenons les prestataires de services de paiement (PSP), par le biais de la directive sur les services de paiement dans le marché intérieur dite « DSP 2 » dans sa version adoptée par le Parlement européen le 3 avril 2014. La proposition de directive rappelle dans ses considérants que les PSP sont également soumis aux obligations de notifications notamment prévues dans la directive SRI et dans la proposition de règlement européen sur les données à caractère personnel susmentionnées. Le texte prévoit que « les prestataires de services de paiement signalent sans retard injustifié, tout incident opérationnel majeur, notamment les incidents de sécurité, à l'autorité compétente de l'État membre d'origine du prestataire de services de paiement » (article 85-2) et ce contrairement à la première version du texte qui prévoyait une notification de l'ABE par l'ANSSI (elle-même prévenue via le mécanisme de notification de la directive SRI). Il reviendra à la charge de l'autorité compétente, « dès réception de la

notification » et « sans retard injustifié », de transmettre à l'ABE « les détails importants de l'incident ». Le PSP devrait notifier dans les « meilleurs délais », les utilisateurs des services de paiement « lorsque l'incident de sécurité risque d'avoir un impact sur les intérêts financiers des utilisateurs des services de paiement fournis » et les informer « de toutes les mesures disponibles qu'ils peuvent prendre de leur côté pour atténuer les effets dommageables de l'incident ».

6. Enfin en France, l'article 110 de la loi du 26 janvier 2016 de modernisation de notre système de santé et le décret n°2016-41 26/01/2016 prévoient une notification sans délai à l'Agence régionale pour la santé (ARS) des incidents graves de sécurité des systèmes d'information ayant des conséquences potentielles ou avérées sur la sécurité des soins, sur la confidentialité ou l'intégrité des données de santé ou sur le fonctionnement normal de l'établissement ou du service (Portail http://signalement.social-santé.gouv.fr). L'ARS transmettra ensuite la notification à l'Agence des systèmes d'information partagés de santé (ASIP Santé).

La CNIL a publié récemment un tableau de synthèse :

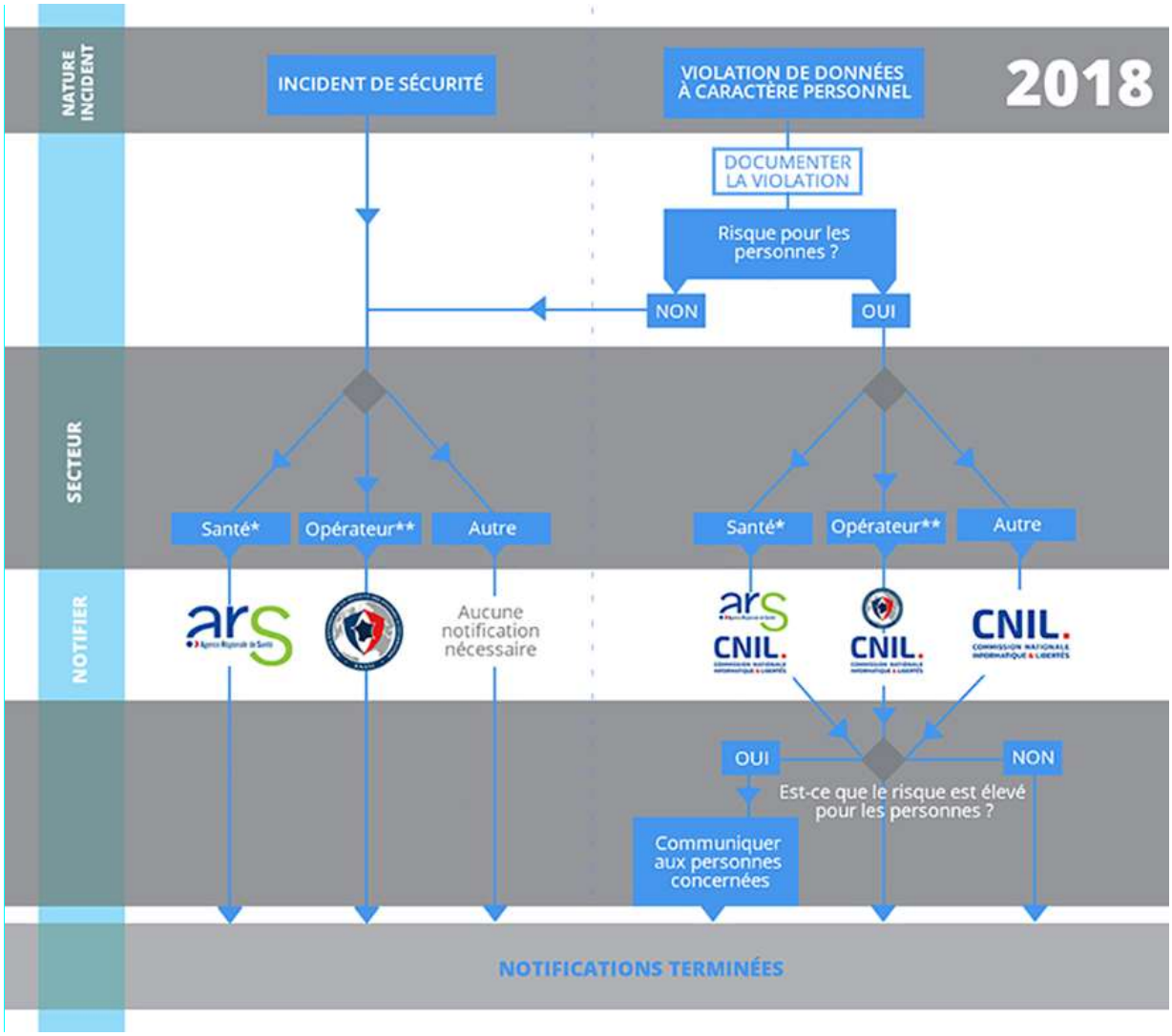


Fig. 10 : déclaration d'un incident de sécurité

* Établissements de santé, hôpitaux des armées, laboratoires de biologie médicale et centres de radiothérapie

*** Opérateur d'importance vitale (OIV), opérateur de service essentiel (OSE) ou opérateur de service numérique (OSN) mettant à disposition des places de marché et les moteurs de recherche en ligne et des services d'informatique en nuage, service de confiance (SDC), ou opérateurs Télécom*

Annexe 2 – Le résumé du cadre réglementaire sur la Sécurité des Systèmes d'information

Rédactrice : Inès Le Lay, sous la direction de Maître Eric Caprioli « *Cyber-Risques et Cyber-Assurance* », Master de droit du Multimédia et de l'Informatique, Dirigé par Monsieur le Professeur Jérôme Passa 2015-2016, Université Paris II, Panthéon – Assas, 58 pages.

L'évolution du cadre légal et réglementaire dans son ensemble va dans le sens de l'exercice de nouvelles responsabilités des opérateurs et d'une nouvelle gouvernance.

Loi informatique et liberté (LI&L), nouveaux articles …

Solvency II, directive 2006/138/CE du Parlement européen et du Conseil du 25 novembre 2009 concerne le monde de l'assurance. A la suite de Bâle II, il s'agit de mieux adapter les fonds propres exigés des compagnies d'assurance et de réassurance aux risques que celles-ci encourent dans leurs activités. Rentrée en vigueur de la directive au 1er janvier 2016. Solvency II exige une maîtrise du portefeuille en imposant que l'assurance soit maîtresse de ses engagements solvables. Si l'assurance doit en effet être capable de justifier de ce qui est souscrit en face de ce qui est indemnisé, les acteurs de la réassurance doivent développer leur compréhension de la quantification – la valorisation pour maîtriser l'agrégation du risque cyber à l'intérieur des programmes en réassurance.

La LPM, loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2016 introduit des mesures générales de sécurité pour les SI pour les Opérateurs d'importance vitale (OIV). Voir également la liste des décrets d'application. **L'article 22** « relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale » du 18 décembre 2013 qui intègre un article L.1332-6-2 au Code de la défense qui prévoit à la charge des Opérateurs d'importance vitale et « des opérateurs publics ou privés qui participent à ces systèmes » l'obligation de respecter à leurs frais des règles de sécurité particulières, mais surtout l'obligation de notifier sans délai au Premier ministre « des incidents affectant le fonctionnement ou la sécurité » de leurs SI. La formulation est ici beaucoup plus large.

Le projet de directive SRI (Sécurité des réseaux et de l'Information) résulte d'une initiative de la Commission de 2013 (accord entre le Parlement et le Conseil en 2015) qui a pour objectif d'accroître la sécurité de l'Internet et des réseaux et systèmes informatiques privés sur lesquels reposent les services. La directive imposera aux opérateurs de prendre des mesures de sécurités appropriées afin de gérer le cyber-risque (art. 14). Les acteurs concernés par la directive sont « les opérateurs fournissant des services essentiels ».

Le règlement eIDAS8 (UE) n°10/2014 du Parlement européen et du Conseil sur l'identification et les services de confiance pour les transactions électroniques a été adopté le 23 juillet 2014. Il est applicable en France depuis le 1er juillet 2016.

Le RGPD.

La directive NIS.

La directive Protection des secrets d'affaires 2016/943 du Parlement européen et du Conseil sur la protection des savoir-faire et des informations commerciales non divulguées a été adoptée le 8 juin 2016 et doit être transposée en France d'ici le 9 juin 2018.

La Loi pour une République numérique adoptée le 7 octobre 2016. Loi n°2016-1321.

La Loi Sapin 2 du 9 décembre 2016 – sur l'action en responsabilité pour insuffisance d'actif.

Les dispositions et la doctrine de la CNIL qui distingue l'obligation de notification des failles de sécurité – obligation de résultat – et l'obligation de sécurité obligation de moyen. Néanmoins les exigences de la CNIL étant très fortes , des régulateurs tels que l'AMF… ainsi que la réglementation bancaire – **l'arrêté du 3 novembre 2013** : les entreprises soumises au contrôle de l'ACPR – autorité de contrôle prudentiel et de résolution – ont des obligations de sécurisation de leurs SI (contrôles réguliers (art. 89) et plan de continuité d'activité art.215), de nombreux points doivent figurer au contrat : un niveau de qualité de service, des mécanismes de secours, un droit d'audit des clients, le prestataire de Cloud doit respecter le RGPD.

La directive DSP 2, La directive (UE) 2015/2366 du 25 novembre 2015 concernant les services de paiement dans le marché intérieur impose des exigences en matière de gouvernance de la sécurité, l'évaluation des risques, le suivi et la déclaration d'incidents.

La norme PCI DSS, le PCI Standards Council a développé la norme PCI DSS – Payment Card Industry Data Security le 15 avril 2015.

La Commission a publié en avril 2018, sur « **Liability and IoT** » Staff Working Document on: Liability for emerging digital[67].

[67] Voir https://ec.europa.eu/digital-single-market/en/news/european-commission-staff-working-document-liability-emerging-digital-technologies

Annexe 3 – Assurance d'une infraction ou d'une sanction : la réponse en droit français

Un arrêt du 14 juin 2012 (Cass. civ. 2e, 14 juin 2012, pourvoi n° 11-17.367, Revue des sociétés 2012, p. 637) a pu être interprété comme susceptible de marquer une évolution dans le traitement de l'assurabilité de la sanction administrative en visant non l'ordre public, mais le caractère intentionnel des faits reprochés. En l'espèce, un dirigeant avait été sanctionné par l'AMF pour manquement à l'obligation d'information du public par diffusion d'informations inexactes. La Cour de cassation a validé l'interprétation des juges du fond (confirmée par la cour d'appel) en ce qu'ils avaient considéré que la faute intentionnelle était « exclusive du caractère aléatoire du contrat d'assurance » afin de conclure que la garantie n'était pas due. Il pourrait être soutenu que le fondement est intéressant, dans la mesure où il pourrait marquer une brèche dans le principe de l'inassurabilité d'ordre public qui, jusqu'alors, ressortait de la jurisprudence. Une opinion pourrait consister à affirmer qu'en faisant le choix de ne pas viser l'article 6 du code civil, la Cour a pu souhaiter laisser aux parties l'opportunité de soumettre la question de l'assurabilité de ce type de sanctions aux juges du fond, qui auraient à se prononcer au cas par cas sur la portée de la faute commise et son caractère intentionnel.

Nous ne partageons pas **cette lecture de l'arrêt du 14 juin 2012 car à aucun moment la question de la licéité de la garantie n'a été posée à la Cour de cassation, dans cette affaire**. Seul le caractère intentionnel de la faute de l'assuré était débattu. La Haute juridiction n'a pas pu répondre à une question qui ne lui était pas posée. On comprend d'ailleurs aisément que l'assureur pour dénier sa garantie n'a pas soutenu lui-même la nullité de son contrat ; il aurait ainsi signalé qu'il propose des garanties inapplicables en France. **Cet arrêt permet bien au contraire de faire le point sur l'assurabilité d'une infraction ou d'une sanction en France.**

Il semble impossible d'assurer les conséquences pénales des fautes commises car la sanction pénale doit rester personnelle. En effet, en cette matière, il existe un principe intangible de personnalité de la peine repris à l'article 121-1 du code pénal qui dispose que « nul n'est responsable pénalement que de son propre fait ». Dès lors qu'un contrat contrevient au principe selon lequel la personne déterminée qui doit subir la peine ne peut se voir substituer aucune autre, la validité de son objet est douteuse.

Si l'on exclue que l'assureur puisse fournir un substitut à la peine, la question centrale est, alors, de savoir si la prise en charge d'une amende civile par un assureur constitue l'accomplissement d'une peine par substitution, ce qui est prohibé.

Les auteurs pénalistes affirment que la peine a connu une forte évolution. Aux peines d'emprisonnement et d'amende se sont adjointes d'autres formes de privations ou de restrictions de liberté, telle que par exemple la suspension du permis de conduire (Y. Mayaud, Droit pénal général, 5e éd., PUF, 2015, n° 503). En outre, des sanctions administratives peuvent accompagner des sanctions pénales ; toutes deux agissent bien comme des punitions, l'une pouvant être le complément ou l'accessoire de l'autre. La multiplication actuelle des amendes civiles ou administratives dans une volonté de dépénalisation ne leur fait pas perdre leur nature de peine.

Or la question de l'assurabilité d'une peine n'est pas nouvelle en assurance (F. Leduc, in Traité du contrat d'assurance terrestre, Litec 2008, n° 142 ; L. Mayaux, Le risque assurable, in Traité de droit des assurances, dir. J. Bigot, T. III, Le contrat d'assurance, LGDJ 2002, n° 1104 à 1108). A cet égard, un arrêt ancien est assez éclairant. La question de la nature de « décimes additionnels » à une amende pénale avait été posée à la Cour de cassation (Com. 21 juin 1960, Bull. civ. IV, n° 246 ; RGAT 1961. 53, note A. Besson). La cour d'appel avait estimé que l'assureur de responsabilité civile devait les prendre en charge (Ibid.). La Haute juridiction a censuré les juges du fond en indiquant clairement que les décimes additionnels à l'amende pénale constituaient une peine accessoire qui prenait donc la nature d'une peine (Ibid.). Par ailleurs, il est admis par les auteurs que le contrat d'assurance qui vise à pallier les conséquences du retrait d'un permis de conduire comporte un objet illicite (L. Mayaux, Le risque assurable, préc., n° 1106 ; F. Leduc, préc., n°

142). Le ministère de l'économie et des finances avait interdit en 1992, pour violation de l'ordre public, le contrat permettant de fournir un chauffeur en cas de suspension de permis (L. Mayaux, Le risque assurable, préc., n° 1106 ; F. Leduc, préc., n° 142 et V. G. Defrance, L'ordre public des assurances, Argus 21 févr. 1992, p. 16 s.). Cette jurisprudence et la position adoptée par les pouvoirs publics est éclairante sur la question de l'assurabilité des amendes civiles et administratives. **L'assurance des amendes civiles paraît en France contraire à l'ordre public car elle contrevient au principe de personnalité des peines fussent-elles civiles**. La portée dissuasive des peines administratives serait supprimée si elles devenaient assurables.

Afin de ne pas donner l'illusion aux entreprises qu'elles peuvent s'assurer sur les marchés étrangers contre le risque extorsion ou d'amendes civiles ou administratives (CNIL), qui ensuite s'avèrent impossibles à mettre en œuvre, il serait opportun de modifier le code des assurances et d'insérer à l'article L. 113-1 un alinéa qui porte prohibition de l'assurance des infractions de même que celle de l'assurance des sanctions pénales, des amendes civiles et administratives.

Annexe 4 – Note sur l'assurabilité des amendes administratives

Au cours des dernières années, le législateur a considérablement accru les contraintes administratives pesant sur les entreprises dans de multiples domaines visant la protection des données, la lutte contre la corruption, le devoir de vigilance, etc.

Qu'il s'agisse de la création de nouvelles autorités régulatrices (telle que l'AFA) ou bien du renforcement des pouvoirs d'investigation ou de sanction d'autorités existantes (telle que la CNIL), la question de l'assurabilité des amendes administratives s'est ainsi retrouvée au cœur de nombreux débats juridiques touchant différentes catégories de garanties, notamment concernant celles dédiées à la couverture des cyber-risques ou de la responsabilité des Dirigeants.

La délivrance par certains assureurs de garantie des amendes dites administratives « sous réserve de leur assurabilité », conjuguée au manque de directive claire du régulateur sur ce sujet ont ainsi engendré une certaine insécurité juridique dans la réelle portée des engagements pris ainsi qu'une apparente distorsion de concurrence entre des acteurs pourtant soumis en théorie aux mêmes réglementations d'ordre public.

L'analyse de la doctrine, de la jurisprudence et de droits comparés permettent néanmoins d'éclairer cette question à l'aube de l'entrée en vigueur de sanctions dont la nature apparaît de plus en plus délicate à appréhender.

Au-delà de toute initiative législative ou réglementaire, les pouvoirs publics et/ou l'autorité de contrôle des assurances se doivent de mener cette analyse afin d'éclairer les assureurs et leurs clients sur le champ du possible en matière d'assurabilité.

Annexe 5 – Avant-projet de réforme du droit des obligations (septembre 2005)

Articles 1101 à 1386 du Code civil – les dommages-intérêts

Les principales innovations prévues concernent les dommages-intérêts punitifs qui sont autorisés à certaines conditions (article 1371), la possibilité de réduire l'indemnisation lorsque la victime n'a pas fait preuve d'une diligence suffisante pour réduire le dommage ou en éviter l'aggravation (article 1373) ainsi que l'obligation pour le juge d'évaluer distinctement chacun des chefs de préjudice allégués (article 1374) et la possibilité qui lui est reconnue, dans des circonstances particulières, d'affecter les dommages-intérêts à une mesure de réparation spécifique (article1377).

- Art. 1370

Sous réserve de dispositions ou de conventions contraires, l'allocation de dommages-intérêts doit avoir pour objet de replacer la victime autant qu'il est possible dans la situation où elle se serait trouvée si le fait dommageable n'avait pas eu lieu. Il ne doit en résulter pour elle ni perte ni profit.

- Art. 1371

L'auteur d'une faute manifestement délibérée, et notamment d'une faute lucrative, peut être condamné, outre les dommages-intérêts compensatoires, à des dommages-intérêts punitifs dont le juge a la faculté de faire bénéficier pour une part le Trésor public. La décision du juge d'octroyer de tels dommages-intérêts doit être spécialement motivée et leur montant distingué de celui des autres dommages-intérêts accordés à la victime. Les dommages-intérêts punitifs ne sont pas assurables.

- Art. 1372

Le juge évalue le préjudice au jour où il rend sa décision, en tenant compte de toutes les circonstances qui ont pu l'affecter dans sa consistance comme dans sa valeur, ainsi que de son évolution raisonnablement prévisible.

- Art. 1373

Lorsque la victime avait la possibilité, par des moyens sûrs, raisonnables et proportionnés, de réduire l'étendue de son préjudice ou d'en éviter l'aggravation, il sera tenu compte de son abstention par une réduction de son indemnisation, sauf lorsque les mesures seraient de nature à porter atteinte à son intégrité physique.

- Art. 1374

Le juge doit évaluer distinctement chacun des chefs de préjudice allégués qu'il prend en compte. En cas de rejet d'une demande relative à un chef de préjudice, le juge doit motiver spécialement sa décision.

- Art. 1375

Si la victime établit qu'un chef de préjudice n'a pas fait encore l'objet d'une demande de sa part ou que son dommage s'est aggravé, elle peut obtenir en tout état de cause une réparation complémentaire, le cas échéant par l'introduction d'une action nouvelle.

- Art. 1376

L'indemnité peut être allouée au choix du juge sous forme d'un capital ou d'une rente, sous réserve des dispositions de l'article 1379-3.

- Art. 1377

Sauf circonstances particulières justifiant l'affectation par le juge des dommages-intérêts à une mesure de réparation spécifique, la victime est libre de disposer comme elle l'entend des sommes qui lui sont allouées.

Annexe 6 - Bibliographie

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

Allemagne

1. BIGS – Brandenbourg Institute for Society and Security, « *Cyber Insurance as a Contribution to IT Risk Management, An analysis of the Market for Cyber Insurance in Germany* », December 2017, https://www.bigs-potsdam.org/images/PP_No7_Cyber%20Insurance.pdf

Belgique

2. FERMA – ECIIA, « *At the junction of Corporate governance and cybersecurity* », http://www.ferma.eu/exclusive-ferma-eciia-cyber-risk-governance-report-available?type=advocacy

France

3. AFDIT, « Panorama d'actualités du droit de l'économie numérique », Paris, 4 juin 2015.
4. AFDIT, « E-reputation : la réputation à l'épreuve du numérique : la gestion en entreprise, les atteintes aux contenus état des lieux, gestion pratique, recours légaux », Paris, 29 octobre 2015.
5. Nicolas SCHIMEL, Banque de France, Revue de la stabilité financière », n° 20, « *Le risque numérique : défi stratégique et opportunité de développement pour les assureurs* », avril 2016.
6. APREF, « *Etude sur les « cyber risques » et leur (ré)assurabilité* », juin 2016, https://www.apref.org/sites/default/files/espacedocumentaire/note_apref_cyber_risque.pdf
7. Frédéric Doche, « *Les données, une mine d'or pour le contrôle de gestion* », Finances et Gestion, la revue d'échanges des dirigeants financiers, n° 342, septembre 2016.
8. Pierre-Luc REFALO, Colloque de la Chaire de Cyberdéfense et Cybersécurité « *Economie de la Cybersécurité* », *Optimisation des dépenses et cyber-assurance*, Paris, 14 novembre 2016.
9. Inès Le Lay, sous la direction de Maître Eric Caprioli « *Cyber-Risques et Cyber-Assurance* », Master de droit du Multimédia et de l'Informatique, Dirigé par Monsieur le Professeur Jérôme Passa 2015-2016, Université Paris II, Panthéon – Assas, 58 pages.
10. CIGREF, « *Valoriser les données de l'entreprise 2020 : maturité, pratiques et modèles* », http://www.cigref.fr/wp/wp-content/uploads/2016/11/CIGREF-Valorisation-des-donnees-Pratiques-Modele-2016.pdf
11. Patrice Cardot, Rapport de force, une collection dirigée par Eric Delbeque et Christian Arbulot, « *Cybersouveraineté, Mythe ou défit ?* », 2016.
12. CIGREF, Charles d'Aumale, François Gratiolet, Stéphane Sollat, François-Xavier Vincent, « Comment débloquer le marché de l'assurance cyber en France ? », juin 2017, http://www.cigref.fr/fil?id=134
13. Emmanuel Sylvestre, « Les sanctions pécuniaires prononcées par les autorités administratives », Lamy des Assurances – 2017.
14. HEXATRUST Cybersecurity & Digital Trust, « *Le guide vers la compliance, un éclairage complet sur la cybersécurite* », édition 2017, www.hexatrust.com
15. Ines Le Lay, sous la direction de Maître Eric Caprioli, « *Cyber-Risques t Cyber Assurance* », Master du droit du Multimédia et de l'informatique, dirigé par Mr le Professeur Jerôme Passa 2015-2016, Université Paris II, Panthéon – Assas.
16. Challenges, « L'essentiel de la sécurité numérique pour les dirigeants », Challenges, 2017.
17. Jean-Laurent Santoni, « Données personnelles, les enseignements de la délibération HERTZ », Expertise Novembre 2017.
18. Rapport de recherche de l'Institut Ponemon, Date de publication, « *Etude annuelle sur la cyber-résilience – 1ère édition pour la France* », février 2017
19. SGDSN, 2017, Chocs Futurs, http://www.sgdsn.gouv.fr/uploads/2017/04/sgdsn-document-prospectives-v5-bd.pdf
20. Jean Lessi, « L'angoisse du RGPD : l'angoisse du RGPD, la CNIL rassure », Expertise, janvier 2018.
21. Le Club des Juristes, Rapport, « *Assurer le risque cyber* », tome 1, le Club des Juristes, commission ad hoc Cyber Risk, janvier 2018.
22. Adoption du projet de loi RGPD, « *Le projet de loi adopté par l'assemblée nationale*», février 2018, https://www.alain-bensoussan.com/avocats/rgpd-gdpr-projet-de-loi-adopte/2018/02/16/
23. SGDSN, « *Revue Stratégique de cyber défense* », février 2018, http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf

Royaume-Uni

24. Lawrence A. Gordon, Martin P. Loeb*,William Lucyshyn, and Lei Zhou, Oxford Academic, Journal of Cybersecurity, *Increasing cybersecurity investments in private sector firms* », 27 November 2015, https://academic.oup.com/cybersecurity/article/1/1/3/2367124
25. Chatham House, Heather M. Roff, « *Advancing Human Security Through Artificial Intelligence* », May 2017, http://weis2017.econinfosec.org/wp-content/uploads/sites/3/2017/06/WEIS_2017_paper_28.pdf

UE

26. Article 29 Data Protection Working Party, 16/EN WP243, « *Guidelines on Data Protection Officers, 'DPO'*», Adopted on December 13th 2016, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048
27. ENISA, « *Commonality of risk assessment language in cyber insurance. Recommandations on Cyber Insurance* », Novembre 2017, https://www.enisa.europa.eu/publications/commonality-of-risk-assessment-language-in-cyber-insurance
28. ENISA, Threat taxonomy,
29. Lloyd's, Emerging Risk Report, « *Costing the Cost, Cyber Exposure decoded* », July 2017 https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/countingthecost
30. Marsh, « *It's time to quantify cyber risk exposure* », http://www.brinknews.com/its-time-to-quantify-cyber-risk-exposure/
31. *City Risk Index 2015-2025*, http://www.lloyds.com/cityriskindex/ Syntheses, https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/city%20risk%20index/city%20risk%20exec%20summary_french.pdf

Suisse

32. Swiss Re Institute, SIGMA No 1/2017, « *Getting to grips with a complex risk* », http://www.swissre.com/media/news_releases/nr20170301_sigma_1_2017.html
33. Swiss Re Institute, SIGMA, No 5/2017, « *Commercial insurance: innovating to expand the scope of insurability* », http://www.swissre.com/sigma/5_2017.html
34. World Economic Forum, Future of Digital Economy and Society Systel Initiative, « *Advancing Cyber resilience, Principles and Tools for the Board* », in collaboration with the Boston Consulting Group and Hewlett Packard Enterprise, January 2017, http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf
35. World Economic Forum, Future of Digital Economy and Society System Initiative, « *Cyber Resilience, Playbook for Public Private Collaboration* », 4.14 Cyber Insurance, http://www3.weforum.org/docs/WEF_Cyber_Resilience_Playbook.pdf
36. CRO Forum Paper 2016, « *Concept Proposal Categorization methodology for Cyber Risk* », concept paper
37. CRO Forum Paper 2018, Supporting on-going capture and sharing of digital event data », Cyber Incident Taxonomy Proposition

USA

38. ACM Conference and Communication, Leyla Bilge, Tudor Dumitras, « *Before we Knew It An Empirical Study of Zero-Day Attacks In The Real World* », 2012, https://users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf
39. Aon Benfield, Cyber Practice Group, Second Issue, « *Cyber Claims Insight* », November 3, 2016, http://thoughtleadership.aonbenfield.com/Documents/20161103-ab-pg-cyber-claims-insight-second-edition.pdf
40. EY, « *Panorama de la Gouvernance 2016, Cap sur l'avenir* ! », http://www.ey.com/Publication/vwLUAssets/EY-panorama-gouvernance-2016/$FILE/EY-panorama-gouvernance-2016.pdf
41. PwC, « Moving Forward with cybersecurity and Privacy, How Organizations are adopting innovative safeguards to manage threats and achieve competitive advantages in a digital area », Key findings from the Global State of Information Security Survey 2017. https://www.pwc.fr/fr/assets/images/2016/10/gsis/GSISS-2017-report-cybersecurity-privacy-safeguards.pdf
42. Deloitte, « *Beneath the surface of a cyberattack A deeper look at business impacts* », https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-beneath-the-surface-of-a-cyber-attack.pdf
43. Rand, Sasha Romanosky, Lillian Ablon, Andreas Kuehn, Therese Jones, 2017 draft, « *Content Analysis of Cyber Insurance Policies: How do carriers write policies and price cyber risk* ? », http://weis2017.econinfosec.org/wp-content/uploads/sites/3/2017/06/WEIS_2017_paper_28.pdf

44. Association of Corporate Counsel, « *Privacy and Data Security : Updates in Privacy and Data Security form 2017 and to Prepare for the Year ahead* », http://www.acc.com/chapters/ncr/index.cfm?eventID=21464
45. Journal of Cyber Policy, Daniel Woods & Andrew Simpson, « *Policy measures and cyber insurance: a framework*, », 2017, http://dx.doi.org/10.1080/23738871.2017.1360927

Agences de notation

46. A report by Lloyds', « *Facing the Cyber Risk Challenge* », 20th September 2016, 22 pages.
47. A.M. Best, Best's Briefing, US Cyber Risk, « *A.M. Best comments on New York States New and Revised Regulation on Cybersecurity* », Regulatory Review, February 17th 2017.
48. Moody's Investor Service, Investor Service, Issuer Comment, « *PlayStation Security Breach is Credit negative for Sony* », 2nd May 2011, 3 pages.
49. Moody's Investor Service, Issuer Comment, « *Sony's second Hack Attack and Security Breach are credit negative*», 9th May 2011, 3 pages.
50. Moody's Investor Service, Investor Service, Global Credit Research, Announcement, « *Moody's sees slow recovery in Sony's profitability as a concern* », 11th July 2011, 3 pages.
51. Moody's Investor Service, Investor Service, Global Credit Research, « USIS security breach is credit negative for Alterity; no impact on rating if federal agencies restore business in short term », 11th August 2014.
52. Moody's Investor Service, Global Credit Research, Rating Action, « *Moody's Downgrade Alterity CFR to Caa3, outlook negative* », 12th September 2014.
53. Moody's Investor Service, Sector in Depth, « *In a major Cyber Attack the Likelihood of Government relief is High* », 15th October 2015, 9 pages.
54. Moody's Investor Service, Sector in Depth, « *Cyber Insurance: High Risk Product with Potential to Grow* », 19th November 2015, 14 pages.
55. Moody's Investor Service, Sector in Depth, Cross Sector Global « *Cyber Risk of Growing Importance to Credit Analysis* », 23rd November 2015, 17 pages.
56. Moody's Investor Services, Sector Comment « US Regulator Approves Cybersecurity Standards, a Credit Positive for Regulated Utilities », 28th January 2016.
57. Moody's Investor Services, Sector In-Depth, « Survey: Bank Boards Engage Growing Cyber Threat, Employ Security-Solution Vendors » 13th July 2016, 12 pages.
58. Moody's Investor Service, Sector in Depth – Cross Sector Global, « *Cyber Risk of Growing Importance to Credit Analysis* », 13th February 2017, 9 pages.
59. Moody's Investor Service, Sector in-Depth, US and Canada Survey « *North American Insurers Step up Cyber Security Initiatives* », 13th February 2017, 9 pages.

OCDE

60. OECD Science, « *Measuring Patent Quality, indicators of technological and economic value, Technology and Industry Working* », Papers 2013/03 https://www.researchgate.net/publication/282877216_Measuring_Patent_Quality_Indicators_of_Technological_and_Economic_Value
61. OCDE, Instruments Juridiques sur les Politiques de l'Économie Numérique, « *Gestion du Risque de Sécurité Numérique pour la Prospérité Économique et Sociale* », 2015, https://www.oecd.org/fr/sti/ieconomie/DSRM_French_final_Web.pdf
62. OECD, Report for the G7 Presidency, « *Supporting an effective cyber insurance market* », 2017, https://www.oecd.org/daf/fin/insurance/Supporting-an-effective-cyber-insurance-market.pdf
63. OECD, Working Party on Security and Privacy in the Digital Economy, « *Review of Surveys on Digital security risk management practices in business* », http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CDEP/SPDE(2017)19&docLanguage=En

Divers

64. ARES, Yulia Cherdantseva, Jeremy Hilton, « A Reference Model of Information Assurance & Security» , 2003 http://users.cs.cf.ac.uk/Y.V.Cherdantseva/RMIAS.pdf

Annexe 7 – La réponse des assureurs et des réassureurs à WannaCry[68]

Le principe indemnitaire traditionnel et le cyber

- **Le logiciel obsolète**

L'assuré utilisant un logiciel obsolète peut-il utiliser sa garantie ou non ? Est-ce que la condition d'octroi de la garantie – la maintenance du système existe ? **Dans la réalisation de l'évènement est-ce que le non maintien est un élément déterminant dans le sinistre**. **Corrélativement, est-ce que l'on est en règle proportionnelle de causalité** ? Si on est dans la condition d'octroi, pas de garantie, puisque l'assuré ne répond pas aux obligations. Si l'assuré est dans la règle proportionnelle de code prime, le jour du sinistre le constat fait est que le système n'est pas celui qui aurait dû être et donc, cette circonstance-là, a entraîné un sinistre tel que si l'assureur avait connu cette situation soit il n'aurait pas délivré sa garantie soit il aurait demandé une prime beaucoup plus importante.

- **Pertinence du questionnaire de l'assureur**

Quel est le lien avec le questionnaire rempli par le client ? **On retombe sur les conditions**, faut-il faire des octrois de condition de garantie ? Ou bien sommes-nous sur le questionnaire et si la question n'a pas été posée, l'assuré peut engager sa garantie.

Qu'est-ce qui doit être compris par maintenance du logiciel ? Soit c'est **une faille 0day**, il est donc difficile de l'opposer à l'assuré. À l'impossible nul n'est tenu et en l'absence de disposition dans le contrat la garantie serait nulle. Soit on est sur un défaut de sécurité, parce que l'assuré n'a **pas patché**. Il y a une vraie question, est-ce que c'est un virus ? Au sens de phénomène reproductible ? Ou un ransomware = quelles sont la qualification de l'objet et la quantification de l'impact. **La qualification de l'objet est-elle nécessaire** ?

- **Le risque juridique des polices devant la Cour de cassation**

La définition d'une garantie sans définition de l'objet n'est pas tenable devant le juge. L'intercalaire de *Marsh* sera challengé par les assureurs au moment du sinistre et par les juges au moment du procès.

La gestion de la crise WannaCry par les assureurs

De nombreux assureurs proposent des services d'aide d'urgence technique à la gestion de la crise aux assurés. Est-ce que ce genre de prestations a été déclenché durant *WannaCry* ?

Les prestations d'assistance des assureurs ont été sollicitées. La prestation d'assistance a été activée. L'assistance technique et juridique mise à disposition par les assureurs de ressources chez le client. *AxA* a fait l'objet de demandes d'information mais aucune activation de mesure d'urgence.

Le besoin de recours à l'assurance aura été très limité.

[68] https://www.ssi.gouv.fr/uploads/.../dossier-de-presse-rapport_annuel-2017_anssi.pdf

Annexe 8 - Présentation succincte des résultats année 1

Le calcul du coût économique et financier d'une attaque cyber pour une organisation portant sur sa chaîne de valeur en lien avec la problématique assurantielle est désormais un sujet incontournable et d'actualité.

Nous constatons aujourd'hui 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. L'absence de recul statistique et de modèles économétriques (peu de recueil statistiques disponible) rend difficile l'évaluation des préjudices liés aux attaques informatiques.

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. Cependant, le secteur de l'assurance identifie dans le marché de l'assurance cyber un potentiel fort de croissance.

De son côté, l'industriel prend la mesure de l'importance du risque cyber et de sa nécessaire maîtrise dans un dialogue constructif avec le monde de l'assurance. Néanmoins, 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. Les organisations privées et publiques commencent à s'interroger sur la définition de leur exposition. Elles peinent à matérialiser leur couverture au risque et s'interrogent sur l'opportunité d'investir dans des couvertures assurantielles cyber au regard des investissements nécessaires à conduire afin de sécuriser leurs systèmes d'information et de protéger leurs infrastructures, leurs produits et leurs données stratégiques. Elles s'interrogent quant au transfert vers l'assurance d'une partie du risque cyber.

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

Une réflexion particulière a été menée sur la réassurance car le cyber-risque s'accompagne de réactions en chaîne susceptibles de toucher la société civile. La crainte d'effets systémiques (impacts sur des chaînes de sous-traitance, atteintes à la réputation, cloud computing, etc.), la rapidité d'évolution des technologies et la fréquence du renouvellement des scénarii d'attaque le font considérer comme **le plus gros risque futur** (territoires intelligents, robotisation croissante, exploitation des données personnelles).

La première année la réflexion a notamment été engagée sur la **définition de l'exposition au risque cyber** afin d'apporter des éléments de réponse de ce qui pourrait constituer un socle partagé par les assurés et les assureurs et réassureurs. Il s'est agi de définir les conditions d'un accord pour définir un cadre de référence en interne (pour l'organisation) et en externe (pour les assurances et les réassureurs) :

- définir et qualifier l'incident cyber du point de vue de l'industriel, de l'assureur et du réassurer ;
- de proposer des critères communs et une méthodologie montrant qu'une organisation répond aux exigences de sécurité face au risque cyber au sens de la loi, mais aussi au sens de la continuité des activités industrielles en cas d'attaque, en réparation et en reprise d'activité ;
- 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 deviendraient les tiers

de confiance qui permettraient la collecte, la validation et l'anonymisation des données, matériaux de base pour la construction des données et la construction des modèles.

Annexe 9 – Les recommandations issues du premier rapport

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***[69] 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.

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 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.

Recommandation3

Une meilleure communication et connaissance des couvertures d'assurance couvrant les conséquences du risque cyber doit être développée. Les *risk managers* et les porteurs des 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

[69] 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.

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.

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[70] 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[71]. 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.

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 :

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

- 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.

Annexe 10 – Tableau de suivi des recommandations (année 1) soit reprises dans d'autres documents soit qui ont fait l'objet d'actions

Les 5 recommandations issues du premier rapport de recherche doivent toujours faire l'effort d'un travail collectif 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.

Recommandations	Actions
Recommandation 1 Chaque entreprise devrait **conduire une analyse financière du risque cyber**	Travaux Année 2 Expérimentation en cours sur la filière aéronautique Idée reprise par l'OCDE
Recommandation 2 Définir un **référentiel et un langage commun**	Action long terme Voir annexe 1
Recommandation 3 **Meilleure communication et connaissance des couvertures d'assurance**	Travaux année 2 : voir chapitre IX Publication par la FFA d'un guide : « Anticiper et minimiser l'impact d'un cyber risque sur votre entreprise : TPE, PME, vous êtes concernées ! »
Recommandation 4 **Gestion de la confidentialité dans le dialogue**	La plateforme https://www.cybermalveillance.gouv.fr/
Recommandation 5 **Normalisation du dialogue et convergence des vocabulaires techniques, assurantiels et juridiques**	Action long terme Voir annexe 2

Fig. 11 : Synthèse de concrétisation des travaux année 1

Annexe 11 – Travaux ultérieurs (année 3)

Les travaux du séminaire année 3 (2018) portent sur la conception et la réalisation d'un exercice cyber s'appliquant à la filière aéronautique et de défense selon une démarche proche de celle développée par l'Université de Cambridge ou des exercices cyber nationaux et internationaux (Piranet, Cyber Europe, Cyber Storm…). La finalité étant de jouer un ou plusieurs scénarios de risque cyber sur l'ensemble de la chaine de la valeur depuis les fournisseurs jusqu'à l'intégrateur final dans le domaine industriel de l'aéronautique et de la défense. Afin de

- comprendre quelle est l'ampleur de ces scénarios pour la supply chain du point de vue du risque manager, de les qualifier et les quantifier financièrement.
- étudier la réponse du marché de l'assurance cyber (courtiers, assureurs, réassureurs) en termes de couverture du risque pour tous les acteurs de la filière : depuis les ETI jusqu'aux grands groupes.
- identifier les domaines assurables et non assurables qui laisseront à la charge de la filière des risques non assurables résiduels pour lesquels elle doit s'organiser.

In fine, la résilience de la chaîne d'approvisionnement face au risque cyber sera analysée en mettant en évidence les grands scénarios de risque catastrophiques d'un point de vue métier et les éventuelles causes systémiques propres à cette filière.

Annexe 12 – La lettre d'invitation

Madame, Monsieur,

Dans le cadre de son projet EIC[72] (Environnement pour l'Interopérabilité et l'Intégration en Cybersécurité), l'IRT-SystemX mène des travaux sur **la maîtrise du risque cyber** dans une approche pluridisciplinaire croisant sciences mathématiques et informatiques avec sciences économiques, sociales et du comportement.

Sous l'impulsion d'**Airbus** et de l'**ANSSI**, l'IRT SystemX anime depuis novembre 2015 un groupe de travail sur « La maîtrise du risque cyber sur l'ensemble de la chaîne de sa valeur et son transfert vers l'assurance ». Il réunit des spécialistes de l'assurance et de la réassurance, des courtiers, des juristes, des actuaires, des industriels (*risk managers*), des experts de l'OCDE sous l'égide de la fédération française de l'Assurance (FFA), de *The Federation of European Risk Management Associations* (FERMA) et de l'association française des professionnels de la gestion des risques et des assurances (AMRAE).

Le travail collectif de ces spécialistes a permis d'examiner :

- les critères communs de définition, de qualification et de quantification du risque cyber ;
- sa couverture assurantielle et les informations de souscription ;
- la gestion du scénario catastrophe.

Une grille d'analyse a également été consolidée. Un **premier rapport de recherches[73]** a été rédigé et publié fin juillet 2016 (en français et en anglais). Il propose 5 recommandations qui ouvrent à de nouveaux travaux.

Nous vous invitons à approfondir ces réflexions en participant à **un deuxième cycle de séminaires** sur la thématique de la **valorisation des biens intangibles** selon le calendrier proposé en Annexe. Les experts d'Airbus, **M. Philippe Cotelle** (Risk Management and Insurance Airbus Defence and Space en charge du risque cyber pour le groupe), **Mme Bénédicte Suzan** (Airbus Defence and Space, R&T and Innovation Coordination) avec l'appui de **M. Philippe Wolf** (Chef du projet EIC) conduiront ces réunions pour en exploiter les résultats. Ces échanges resteront confidentiels.

Plus généralement, **la maîtrise, la quantification et l'assurance du risque numérique** deviennent un impératif pour l'ensemble de la société et donc un facteur de différenciation pour le tissu économique et les entreprises qui le nourrissent. Cela touche aussi bien à la protection du savoir-faire et des biens informationnels des entreprises qu'à la pérennité de leurs activités menacées par des attaques de plus en plus ciblées. **C'est pourquoi nous cherchons de nouveaux partenaires pour un projet de recherche dédié** entre acteurs de la recherche publique et industrielle.

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

Philippe WOLF

[72] Voir http://www.irt-systemx.fr/project/eic/

[73] Voir http://www.irt-systemx.fr/publications/english-la-maitrise-du-risque-cyber-sur-lensemble-de-la-chaine-de-sa-valeur-et-son-transfert-vers-lassurance/

Annexe 13 – L'IRT-SystemX

SystemX est l'un des huit instituts de recherche technologique qui ont été créés par le gouvernement pour renforcer l'attractivité du territoire.

« Un Institut de Recherche Technologique (IRT) est un institut thématique interdisciplinaire qui développe des filières économiques liées à son domaine au travers d'un partenariat stratégique public-privé équilibré. Pour cela, il pilote des programmes de recherche couplés à des plateformes technologiques, effectue des travaux de recherche et de développement au meilleur niveau international, contribue à l'ingénierie des formations initiales et continues (formation professionnelle qualifiante et/ou diplômante) ; et veille à la valorisation des résultats obtenus. »

Lancé en 2012, SystemX, unique Institut de Recherche Technologique (IRT) dédié à l'ingénierie numérique des systèmes du futur, répond aux défis scientifiques et technologiques de l'industrie et des territoires au moyen d'une innovation flexible, ouverte et collective.

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

- La colocalisation de ses talents. L'institut réunit au sein d'un même lieu tous les partenaires des projets, permettant ainsi de créer un véritable creuset d'interactions entre acteurs de la recherche publique et industrielle.
- La mutualisation des compétences et des plateformes. L'IRT SystemX consolide des plateformes technologiques grâce à la mise en commun de composants et d'infrastructures issus des projets de recherche, et développe des expertises, au service de ses partenaires publics et privés.

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.

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 14 – 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.

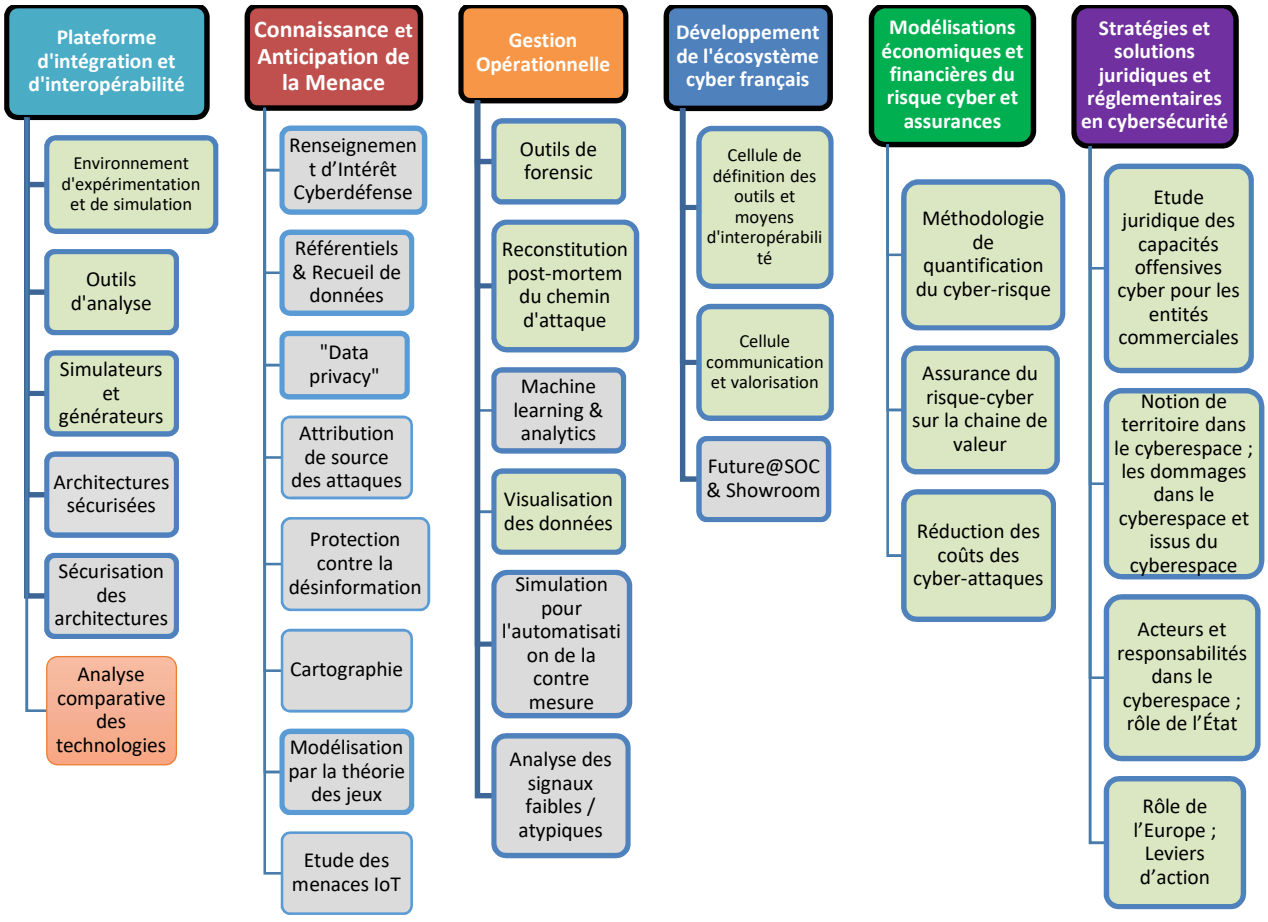


Figure 11 : décomposition du programme de recherche EIC en tâches et sous-tâches

Airbus 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). 2017, publication du premier rapport de recherche sur les conditions du transfert du risque cyber d'une organisation vers le marché. 2018, publication du second rapport de recherche sur la valorisation des données intangibles en vue de leur transfert vers le marché de l'assurance. 2018, troisième séminaire de recherche sur le transfert du risque cyber sur la chaine de la valeur de la supply chain de l'aéronautique et de défense.

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).

Annexe 15 – Les 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 seconde année de notre programme de recherche. Cette liste n'est pas exhaustive.

Administrateur	
Agences de notation A.M. BEST Moody's	
Assureurs AIG AXA Entreprise ; Groupama ; Liberty Mutuel; Les Lloyds.	**Réassureurs** Hannovre-re Libertyglobalgroup Munich-Re France Partner-re SCOR SIRE Swiss-re
Courtiers Clevercourtage Marsh	
Associations professionnelles APREF FERMA-AMRAE FFA Institut des actuaires	
Cabinet de commissaires aux comptes Ernest&Young	**Cabinet de juristes** KGA-Avocats.
Cabinet experts judiciaires ICA-ICSI	
Industriels, PME Airbus Group LINEON	
Organisations internationales OCDE (2 départements) UE – ECSO PPP	**Ministère de l'Économie, de l'Industrie et du Numérique** ACPR – Banque de France ; Direction générale des entreprises (DGE) ; Direction générale du Trésor, Sous-direction des Assurances ; Conseil général de l'économie (CGE) : section Sécurité et Risques.
SGDSN / ANSSI	
IRT SystemX	

Annexe 16 – Groupe de travail

Liste nominative des participants.

Allaire Olivier	olivier.allaire[at]lineon.fr
Badiane Laurent	lbadiane[at]kga.fr
Beaume François	francois.beaume[at]bureauveritas.com
Bejuy Hélène	h.bejuy[at]ffsa.fr
Bernat Laurent	laurent.bernat[at]oecd.org
Bing Pierre-Yves	pierresvesbing[at]dfcg.asso.fr
Boisard Anne-Sophie	asboisard[at]cigref.fr
Bourgeois Matthieu	m.bourgeois[at]kga.fr
Canameras Gilbert	gilbert.canameras[at]erametgroup.com
Célérier Laurent	laurent.celerier[at]ssi.gouv.fr
Chapron Stanislas	stanislas.chapron[at]marsh.com
Clayton Laurence	l.clayton[at]lca-icsi.com
Cotelle Philippe	philippe.cotelle[at]astrium.eads.net
Crochemore David	david.crochemore[at]ssi.gouv.fr
Danilo D'Elia	danilo.delia[at]ecs-org.eu
Daubignard Cécile	cecile.daubignard[at]groupama.com
Daviot Christian	christian.daviot[at]ssi.gouv.fr
De Jabrun Xavier	xavier.dejabrun[at]thalesgroup.com
De La Rochefoucauld Guy-Antoine	guy-antoine-delarochefoucauld[at]lloyds.com
De Mercey Laurent	laurent.de-mercey[at]finances.gouv.fr
Defransure Jean-Paul	jean-paul.defransure[at]mbda-systems.com
Delcamp Christophe	c.delcamp[at]ffsa.fr
Desoblin Gilles	gilles.desoblin[at]irt-systemx.fr
Dollfus Bénédicte	benedicte.dollfus[at]wanadoo.fr
Ducrot Gisèle	gisele.ducrot[at]fr.ey.com
Duflot Loïc	loic.duflot[at]finances.gouv.fr
Elbilia Michel	michel.elbilia[at]covea.fr
Flepp Gilbert	gilbert.flepp[at]acegroup.com
Gaillard Philippe	philippe.gaillard[at]axa.fr
Gardin Denis	denis.gardin[at]mbda-systems.com
Grégoire St Marie Caroline	caroline.gregorestemarie[at]gmail.com
Groh Thomas	thomas.groh[at]gdtresor.gouv.fr
Guibert Silvestre	jose.guibert[at]groupama.com
Héon Sébastien	sheon[at]scor.com
Kociemba Marine	m.kociemba[at]ffa-ssurance.fr
Laflandre Philippe	philippe.laflandre[at]airbus.com

Laurent Rosy	rosy.laurent[at]apref.org
Le Cam Ghislain	ghislain.lecam[at]ambest.com
Lemaire Jean-Raymond	jr-lemaire[at]lca-icsi.com
Madinier Charles-Henry	charles-henry.madinier[at]marsh.com
Maia Jean	jean.maia[at]finances.gouv.fr
Martinon David	david.martinon[at]diplomatie.gouv.fr
Monmoton Olivier	olivier.monmoton[at]hannover-re.com
Oger Severine	severine.oger[at]ssi.gouv.fr
Parisot Sophie	sophie.parisot[at]aig.com
Parsoire Didier	dparsoire[at]scor.com
Pépin Jean-François	jean-francois.pepin[at]cigref.fr
Picard Florence	florencepicard[at]aol.com
Plumerand Shirley	shirley.plumerand[at]gmail.com
Pouillot Patrick	ppouillot[at]munichre.com
Reboul Yannick	yannick.reboul [at]edf.fr
Ribera Alain	alain.ribera[at]airbus.com
Richard Patrick	patrick.richard[at]swissre.com
Rolin Elizabeth	elisabeth.rolin[at]ssi.gouv.fr
Ronchi Elettra	elettra.ronchi[at]oecd.org
Roure Françoise	francoise.roure[at]finances.gouv.fr
Santoni Jean-Laurent	jean-laurent.santoni[at]clevercourtage.com
Santucci Gérald	gerald.santucci[at]ec.europa.eu
Silvestre Emmanuel	emmanuel.silvestre[at]libertyglobalgroup.com
Simonel Laurent-Xavier	lx.simonel[at]kga.fr
Spalacci Stéphane	s.spalacci[at]ffsa.fr
Suzan Bénédicte	benedicte.suzan[at]airbus.com
Thierry Moreau	thierry.moreau[at]fr.ey.com
Vignancour Luc	luc.vignancour[at]marsh.com
Vignial Cécile	cecile.vignial[at]oecd.org
Warzee Didier	didier.warzee[at]acpr.banque-france.fr
Wendling Cécile	cecile.wendling[at]axa.com
Wyka Virginie	virginie.wyka[a]partnerre.com
Wolf Philippe	philippe.wolf[at]irt-systemx.fr

-_-_-_-_-_-