IRM | institut du risk management

Rapport de projet présenté devant un Jury de Soutenance

Expert ERM

Expert(e) Management des Risques Financiers et Assurantiels

Le 18/11/2021

Par : Jean-Philippe MOINEAU & Rostand TAGNE WAMBO

Titre : Gestion du risque Cyber dans une entreprise d'assurance par une approche ERM

Confidentialité : ☒ NON ☐ OUI (Durée : ☐ 1an ☐ 2 ans)

La durée de confidentialité expire aux 31 décembre N+1 (1 an) ou N+2 (2 ans)

Les stagiaires s'engagent à ce que les données de l'Entreprise présentées dans le cadre des travaux de la formation (rapport de projet & présentation) respectent les règles relatives à la protection des données à caractère personnel conformément aux dispositions de la Loi informatiques et Liberté n°78-17 du 6 janvier 1978 modifiée par la Loi du 6 août 2004 ainsi que par la loi n° 2018-493 du 20 juin 2018 (RGPD)

Membres présents du jury :

_____

_____

_____

_____

_____

_____

Par ma signature j'autorise la publication sur un site de diffusion de documents actuariels du rapport de projet
(après expiration de l'éventuel délai de confidentialité)

Nom : MOINEAU

Prénom : Jean-Philippe

Signature du stagiaire

Si binôme :

Nom : TAGNE WAMBO

Prénom : Rostand

Signature du stagiaire

Gestion du risque Cyber dans une entreprise d'assurance par une approche ERM

Jean-Philippe MOINEAU – Rostand TAGNE WAMBO

Table des matières

1. Introduction

1.1. Préambule

La notion de « Enterprise Risk Management » (ERM) peut revêtir différentes définitions. Le cadre de l'ERM défini dans le COSO[1] (mise à jour de 2016), considère l'ERM comme « la culture, les capacités et les pratiques, intégrées à la définition de la stratégie et à son exécution, sur laquelle les organisations s'appuient pour gérer le risque dans la création, la préservation et la réalisation de valeur ».

Nous voyons ici que les notions « gestion des risques » et « valeur de l'entreprise » relèvent d'un intérêt majeur dans cette discipline.

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)[2], s'attache régulièrement à rappeler le lien étroit entre sécurité économique et sécurité numérique pour une entreprise. Les rançongiciels, tels que WannaCry ou NotPetya, dont les noms, évocateurs pour certains, rappellent des attaques mondiales perpétrées en 2017, en sont des exemples concrets. L'ampleur de ces attaques informatiques, d'un niveau « sans précédent »[3], dépasse les simples dommages informatiques et a fait prendre conscience que le scénario d'un virus informatique provoquant la faillite d'une entreprise ne relevait plus de la simple théorie.

Nous voyons bien là l'intérêt à développer une gestion des risques informatiques afin de préserver la « valeur » de l'entreprise.

1.2. Les risques informatiques : définition du risque « Cyber »

La gestion des risques informatiques peut aller bien au-delà de la protection contre les activités de malveillance. En effet, elle englobe également tout l'écosystème digital dans l'absolu : gestion de la donnée, des sauvegardes, disponibilité des outils, maintenance des solutions informatiques, etc. ; il s'agit de la gestion de l'ensemble du système des technologies de l'information. S'intéresser à ce risque dans son ensemble ne peut nécessairement pas s'inscrire dans le cadre de ce rapport.

Nous nous intéresserons ici au sujet « Cyber », pour lequel, afin de définir le cadre, nous apportons les définitions suivantes :

- **Cyberattaques** : ce sont des tentatives, abouties ou non, visant à obtenir un accès non autorisé à des informations ou à des systèmes d'information, afin de voler ou de modifier des informations ou de bloquer des systèmes informatiques[4] ;

[1] Le COSO est un référentiel de contrôle interne défini par le *Committee Of Sponsoring Organizations of the Treadway Commission*.

[2] Créée en 2009, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est un service à compétence nationale rattaché au secrétariat général de la Défense et de la Sécurité nationale (SGDSN, autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale). Elle a notamment pour mission de mettre en œuvre des dispositifs de détection, lors d'événements susceptibles d'affecter la sécurité des systèmes d'information de l'Etat, des autorités publiques et d'opérateurs publics et privés, ainsi que le recueil d'informations techniques relatives à ces incidents, et l'accompagnement pour y répondre.

[3] Telle que qualifiée par Europol, l'agence européenne spécialisée dans la répression de la criminalité.

[4] AICA (2019) Cyber Risk in the Insurance Sector

- **Cyber-risque** ou « **risque Cyber** » : c'est la combinaison de la probabilité qu'une cyberattaque se produise, susceptible d'engendrer des dommages causés par ce type de cyberattaque[5] ;
- **Cybersécurité** : elle désigne quant à elle la « préservation de la confidentialité, de l'intégrité et de la disponibilité des informations et/ou des Systèmes d'Information (SI) par l'intermédiaire d'un dispositif de sécurité »[6].

Dans le cadre de ce rapport, nous nous intéresserons donc à la gestion du risque Cyber par une approche ERM.

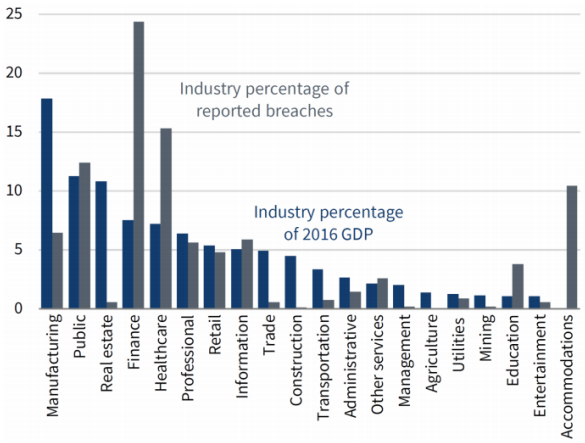
1.3. Le risque Cyber pour une entreprise d'assurance

L'usage généralisé de l'informatique, pour toutes entreprises quelles qu'elles soient, induit que chacune d'entre elles peut être sujette à des cyberattaques :

- les entreprises de taille intermédiaire (ETI) ou très grandes entreprises (TGE) vont être la cible de hackers expérimentés, intéressés par le gain potentiel de leurs attaques. Elles vont également être exposées en raison de leurs compétences ou expertise dans des domaines particuliers (cf. espionnage industriel) ;
- les petites et moyennes entreprises (PME), moins exposées médiatiquement que les ETI ou TGE, sont également exposées au risque Cyber : du fait de leur dimension, leurs potentielles faibles mesures de sécurité mises en place (ex. pas de Direction des Systèmes d'Information interne), elles seront des cibles plus « faciles » pour hackers (qui de fait, ne sont pas nécessairement très expérimentés, donc en plus grand nombre).

L'évolution du nombre de cyberattaques ces dernières années, de plus en plus organisées et ciblées, accentuée par un recours important au télétravail dû aux mesures de confinements mises en place à travers le monde (suite à la crise sanitaire Covid-19), a contribué à renforcer l'idée que le risque de cyberattaques est une menace croissante.

Un rapport du Council of Economic Advisers (*The Cost of Malicious Cyber Activity to the U.S. Economy* [7], Février 2018) mettait par ailleurs en évidence que les secteurs de la finance et de la santé étaient les plus exposés aux cyberattaques du fait de la valeur des données qu'ils détiennent sur leurs clients. En effet, le graphe ci-contre, extrait de ce rapport, met en parallèle la contribution au PIB américain des différentes industries *(en bleu)* et la répartition des cyberattaques qu'elles subissent *(en gris)*.



Source : The council of Economic Advisers (2018), The Cost of Malicious Cyber Activity to the U.S. Economy

[5] Cyber Lexique FSB (2018)
[6] Définition ACPR (Notice relative à la sécurité et à la gouvernance des technologies de l'information et de la communication)
[7] https://trumpwhitehouse.archives.gov/articles/cea-report-cost-malicious-cyber-activity-u-s-economy

D'évidence, les assureurs sont des acteurs majeurs dans ces deux secteurs. En effet, les assureurs recueillent, stockent et traitent des volumes importants de données personnelles et commerciales confidentielles et donc hautement sensibles. Parce qu'ils disposent de ces imposantes banques de données, les assureurs deviennent des cibles privilégiées au regard des cyberattaques. En outre, parce que les assureurs contribuent grandement au secteur financier mondial, toute interruption des systèmes d'assurance causée par des incidents en matière de cybersécurité peut avoir des répercussions considérables.

L'exemple récent de l'attaque au rançongiciel à l'encontre de CNA Financial (mars 2021), acteur majeur dans l'industrie de l'assurance aux Etats-Unis et contraint à payer une rançon de 40 millions de dollars afin de retrouver l'accès à ses systèmes, met en évidence l'intérêt que des cybercriminels peuvent porter au secteur assuranciel. En France, nous pouvons également noter les récentes attaques subies par l'assureur mutualiste MMA (juillet 2020), la Mutuelle nationale des hospitaliers (MNH, février 2021) ou encore le courtier AssurOne, filiale du groupe Prévoir, qui a été contraint en août 2021 de mettre une partie de ses serveurs à l'arrêt. En cause, la tentative de « ransomware » (rançongiciel) mené par Ragnorak, un groupe de hackers connu pour avoir notamment attaqué de grands groupes comme l'éditeur Citrix.

Les cyberattaques s'intensifiant, et les secteurs de la finance et de la santé étant les plus exposés, c'est tout naturellement que, dans la cartographie prospective établie par la FFA[8], le risque de cyberattaques létales (i.e. de grande ampleur avec mise à l'arrêt du SI de l'entreprise) est identifié comme étant la principale menace pour les sociétés d'assurance et de réassurance ; une position inchangée depuis 4 ans.

Par voie de conséquence, le risque Cyber dans le secteur de l'assurance fait l'objet d'une attention particulière de la part des autorités de contrôle :

- L'AICA[9], dans son document de réflexion[10] sur le risque Cyber dans le secteur, stipule que les risques en matière de sécurité informatique sont une menace grandissante pour le secteur des assurances, et qu'en vertu des principes de base d'assurance, les autorités de contrôle n'ont pas d'autre choix que de contre-attaquer ;
- L'ACPR, pour sa part, incite les entreprises d'assurance à améliorer leur gestion du risque Cyber. En juillet 2021, l'autorité a publié une notice relative à la sécurité de l'information et à la gouvernance des Technologies de l'information et de la communication (TIC) à destination des entreprises d'assurance ou de réassurance relevant du régime « Solvabilité II »[11], en lien avec les orientations de l'EIOPA publiées en octobre 2020[12]. Sur le plan des principes, cette notice souligne que **le risque informatique mérite d'être pleinement pris en compte dans le dispositif général de gestion des risques.**

---

[8] Cartographie prospective 2021 des risques de la profession de l'assurance et de la réassurance : https://www.ffa-assurance.fr/la-federation/publications/barometre-des-risques-emergents/cartographie-prospective-2021-des-risques

[9] L'Association internationale des contrôleurs d'assurance plus connue sous son acronyme anglais IAIS (International Association of Insurance Supervisors).

[10] Consultable à l'adresse suivante : https://www.iaisweb.org/page/supervisory-material/issues-papers/file/61857issues-paper-on-cyber-risk-to-the-insurance-sector

[11] https://acpr.banque-france.fr/sites/default/files/media/2021/07/02/20210702_notices_orientations_aeapp.pdf

[12] https://www.eiopa.europa.eu/document-library/guidelines/guidelines-information-and-communication-technology-security-and_en

2. Démarche ERM

2.1. Cadre de l'étude

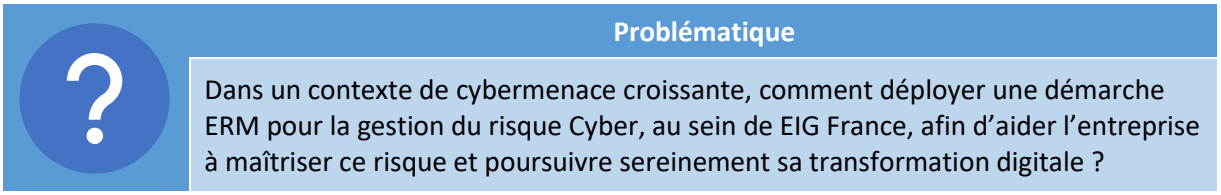
Nous nous plaçons dans le cadre d'un grand groupe d'assurance international fictif que nous nommons EIG (« European Insurance Group »). Le Groupe EIG opère, via ses filiales (appelées « entités » et dirigées par un unique Corporate Center[13]), sur les 5 continents, avec une forte présence en Europe. EIG offre une gamme complète de produits afin de répondre au mieux à l'ensemble des besoins de ses clients et leur offrir la meilleure expérience d'assurance.

Dans notre étude nous nous intéressons à EIG France, l'entité française de EIG. A l'image du groupe, elle propose une gamme complète des produits d'assurance : assurance de biens et responsabilité, santé et prévoyance, épargne et retraite.

Avec l'arrivée de son nouveau Directeur Général, EIG France connait un fort développement de son chiffre d'affaires ces dernières années et une transformation digitale importante de ses activités. L'entité, dont la vente des produits se faisait principalement par son réseau traditionnel (agents généraux), a diversifié ses canaux de distributions avec la vente en ligne, qui représente désormais une part importante de son chiffre d'affaires (20%) et continue de progresser. De plus, elle a développé de nouveaux partenariats avec des courtiers, y compris des courtiers en ligne, et les sites de comparateur de produits d'assurance.

Tandis que le nombre de cyberattaques observées ces dernières années est en croissance, intensifiée par la généralisation du télétravail, une des filiales européennes de Groupe EIG a été victime d'une cyberattaque en début d'année.

À la suite de cette attaque et compte tenu de la transformation digitale de EIG France, le Corporate Center a souhaité avoir une vision claire du niveau de maîtrise de l'entité vis-à-vis du risque Cyber. Cette demande répond aussi à une attente de son Directeur Général qui souhaite poursuivre sereinement la transformation digitale de son entité.



A cette fin, une mission est menée conjointement par la Direction des risques de EIG France et celle du Corporate Center.

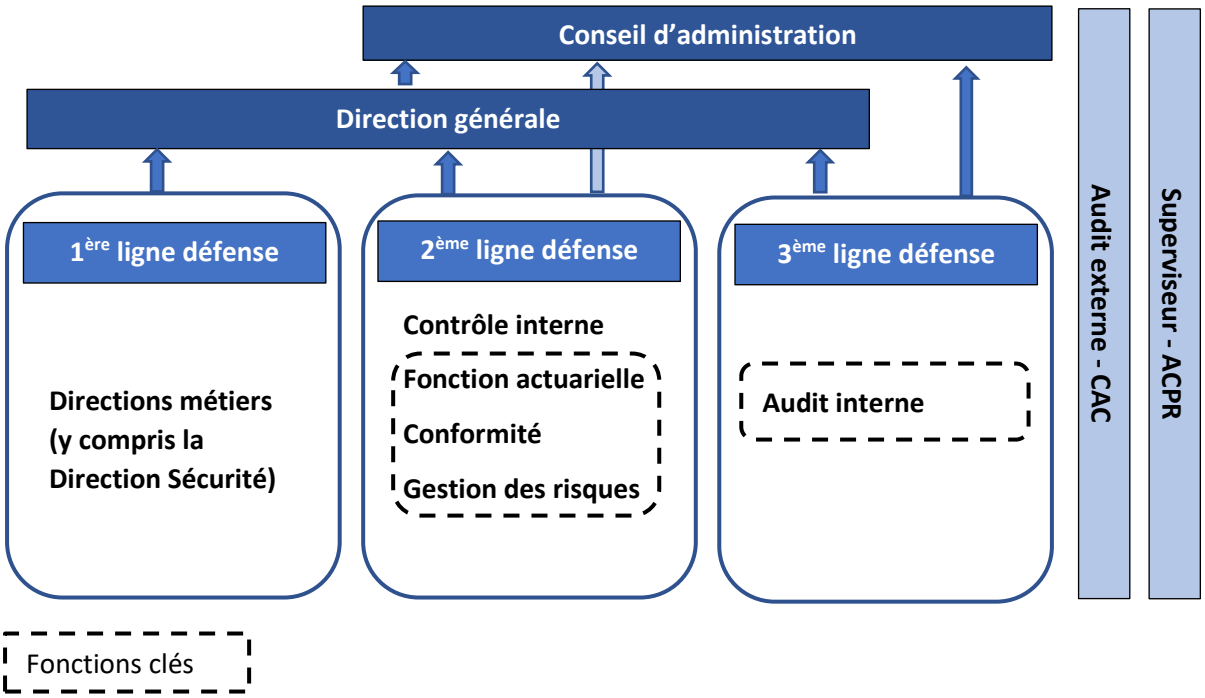
2.2. Système de gestion relatif au risque opérationnel

L'article 44 de la directive Solvabilité II décrit le système de gestion des risques que doivent mettre en place les entreprises d'assurance. Ce système doit couvrir au moins six domaines[14] dont la gestion du risque opérationnel.

[13] Chaque responsable local (i.e. en entité) de fonctions régaliennes (CFO, CRO, Actuarial Function Holder, etc.) reporte à 50% à son homologue du Corporate Center.

[14] La souscription et le provisionnement, la gestion actif-passif, les investissements, en particulier dans les instruments dérivés et engagements similaires, la gestion du risque de liquidité et de concentration, la réassurance et les autres techniques d'atténuations, la gestion du risque opérationnel.

Ces dispositifs sont bien mis en place au sein de EIG France, où la gestion du risque Cyber est intégrée au système de gestion du risque opérationnel. Ce dernier s'intégrant au dispositif global de gestion des risques de EIG France, organisé en trois lignes de défense.



Toutes les équipes de l'entité constituent la première ligne de défense. En effet, la maitrise du risque opérationnel fait partie intégrante des missions de l'ensemble des collaborateurs. Sur le risque Cyber en particulier, la Direction Sécurité a une responsabilité de pilotage et de mise en place des moyens de remédiation sur ce risque ; son rôle est essentiel afin que l'environnement de contrôle soit plus effectif et moins vulnérable à des menaces externes.

La deuxième ligne de défense est assurée notamment par le Contrôle Interne, qui s'assure que les contrôles opérationnels sont effectifs, la Fonction actuarielle, la Fonction de vérification de la conformité ainsi que la Gestion des risques qui définit la gouvernance à appliquer. Là où la première ligne de défense a un rôle de mise en œuvre des moyens de remédiation pour s'assurer que le risque Cyber est maitrisé, la deuxième ligne, quant à elle, a un rôle de surveillance de ce risque.

La direction de l'Audit interne assure la troisième ligne de défense. Elle réalise une évaluation périodique de l'efficacité des dispositifs mis en place pour la gestion du risque.

Le suivi du dispositif de gestion des risques opérationnels est assuré par le comité des risques opérationnels qui couvre le risque opérationnel, mais également les risques de conformité et de réputation. Le comité se réunit bimestriellement et a pour participants :

- Le Directeur Général de EIG France qui assure la présidence ;
- Le responsable des opérations ;
- Le responsable de la gestion des risques ;
- Le responsable du risque opérationnel et du Contrôle Interne ;
- Le responsable de la Conformité ;
- Le responsable de la Sécurité des Systèmes d'Information (RSSI) ;
- Le responsable des Ressources Humaines ;
- Le responsable de la Communication.

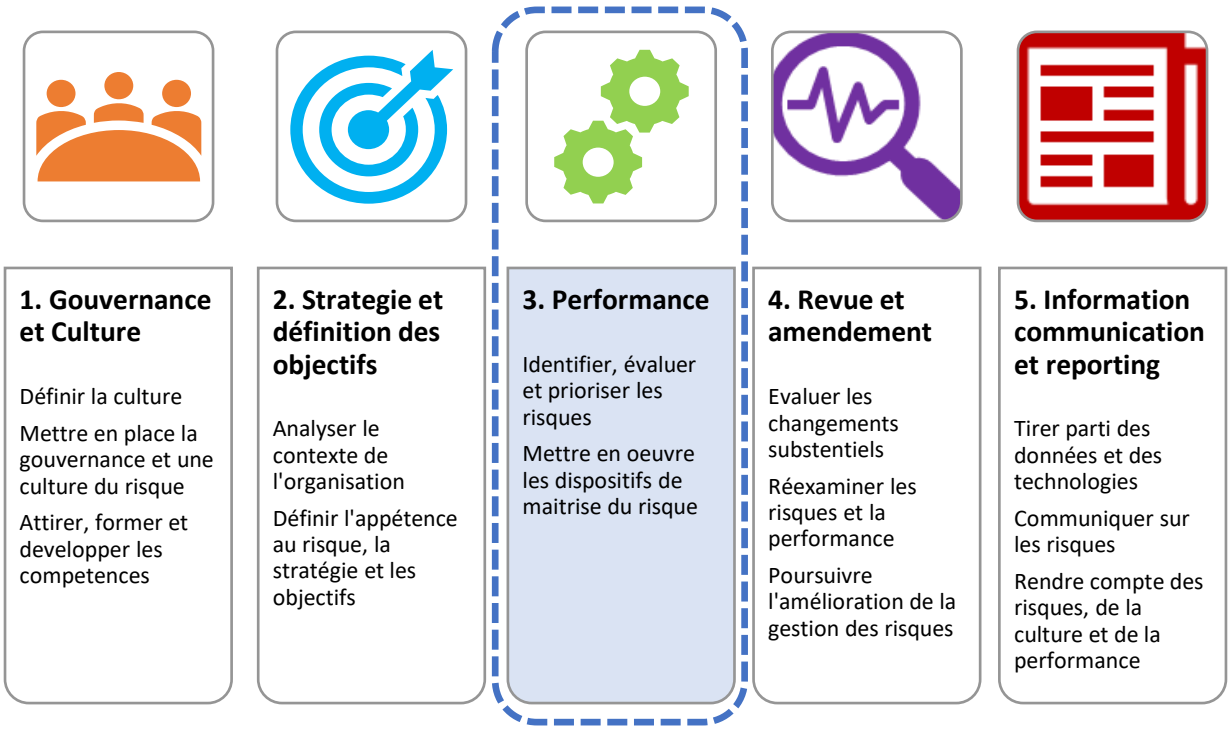
2.3. Référentiel COSO

Dans l'entreprise, la gestion du risque Cyber est une activité complexe, avec une composante technique, humaine et organisationnelle. Afin de pouvoir l'aborder sous toutes ses facettes, il est utile de partir de références permettant d'apporter principes et idées afin de couvrir à minima les questions essentielles. Le COSO est le référentiel que nous utiliserons pour la gestion de ce risque.

C'est un référentiel qui existe depuis 1992 et défini par le Committee Of Sponsoring Organizations of the Treadway Commission. Sa dernière mise à jour date de 2017. Cette version du COSO ERM vise à refléter les enjeux suivants :

- Transparence et fiabilité demandées par les parties prenantes ;
- Contexte de plus en plus complexe, axé sur les nouvelles technologies ;
- Prise de conscience suite aux incidents (crises, attaques, cybercriminalité, etc.).

Le cadre référentiel s'articule autour de cinq composantes interdépendantes :



Dans cette étude, nous nous concentrons sur le déploiement de la **composante 3 « Performance ».** Elle sera déclinée concrètement comme suit :

- L'établissement d'une **cartographie des risques** liée au risque Cyber (section 3) ;
- La description du **traitement des risques** (section 4), en lien avec l'appétit de EIG France pour ce risque, en précisant les contrôles à mettre en place pour en assurer la **surveillance**.

3. Cartographie des risques

La cartographie des risques permet d'appréhender l'ensemble des facteurs auxquels EIG France est exposée.

Nous détaillons, dans cette partie, la **démarche que nous avons appliquée** pour l'établissement de cette cartographie.

Nous listons ensuite les **risques identifiés pour EIG France**, avant d'indiquer leur **évaluation**.

Cette évaluation a permis leur priorisation, compte tenu de de leur importance. Des mesures d'atténuation ont alors été proposées afin de permettre à EIG France de mieux appréhender son développement dans son environnement. Cela fera l'objet de la partie suivante (cf. section 4).

3.1. Démarche appliquée pour la réalisation de la cartographie

3.1.1. Référentiel utilisé

Dans le cadre de la gestion de ses risques, EIG France utilise un **référentiel interne** (cf. annexe 6.1). Ce référentiel permet d'avoir une **vision globale des risques de EIG France**. Cependant, la partie relative au risque Cyber n'y est pas suffisamment détaillée. D'où la nécessité d'**utiliser un référentiel adapté à notre mission**.

Le comité de gestion des risques opérationnels du Corporate Center de EIG (« Group OpRisk Committee ») a diligenté des missions similaires (relatives à la maitrise du risque Cyber) dans plusieurs entités du Groupe. Dans un souci d'efficacité, afin d'harmoniser l'approche et la restitution des missions, **une nomenclature spécifique au risque Cyber a été établie** par le Corporate Center. Celle-ci repose sur la taxonomie proposée par le CRO Forum[15], axée spécifiquement sur les évènements numériques.

Les familles et sous-familles de risques définies dans cette nomenclature sont les suivantes :

Famille	Sous-famille
Fraude interne	Activité non autorisée
	Vol et fraude interne
	Sécurité des systèmes (interne) – Dommages volontaires
Fraude externe	Vol et fraude externe
	Sécurité des systèmes (externe) – Dommages volontaires
Clients, produits et pratiques commerciales	Conformité, diffusion d'informations et devoir fiduciaire
	Pratiques commerciales ou de marché incorrectes
	Activités de conseil
Dysfonctionnements de l'activité et des systèmes	Défaillance du système interne
	Défaillance du système externe
Exécution, livraison et gestion des processus	Saisie, exécution et suivi des transactions

(les définitions détaillées de ces familles et sous-familles sont disponibles en annexes 6.2)

[15] Supporting on-going capture and sharing of digital event data (2018): https://www.thecroforum.org/wp-content/uploads/2018/02/201802_CROF_Capture_and_sharing_of_digital_event_data.pdf

Il est à noter que le risque de réputation, bien que réel et induit par la réalisation de certains des risques qui seront évoqués ci-après, ne fait pas partie de cette nomenclature. La réputation est considérée comme un impact lors de l'évaluation des risques opérationnels identifiés.

3.1.2. Analyse préalable des risques de cyberattaques en France

Avant de démarrer nos travaux d'identification des risques internes à EIG France, nous nous sommes intéressés aux risques de cyberattaques sur le marché français. Un **risque étant la combinaison d'une menace et d'une vulnérabilité**, nous avons cherché à connaitre les **principaux vecteurs** d'une cyberattaque (i.e. menace) d'une part, et les **principales causes d'incident** (i.e. vulnérabilité) d'autre part, sur le marché français.

Une enquête du CESIN (Club des Experts de la Sécurité de l'Information et du Numérique)[16], reporte les principaux vecteurs d'attaques ayant impacté les entreprises françaises (parmi les répondants[17]) en 2020, ainsi que les principales causes. Il en ressort que les **principales menaces** sont les suivantes (détail en annexe 6.3) :

- **Phishing** ou **spear phishing**[18] (80% des répondants ont été impacté) ;
- **Exploitation d'une faille** (52%) ;
- **Arnaque au président** (42%), qui consiste, pour le fraudeur, à contacter une entreprise cible, en se faisant passer pour le président de la société mère ou du groupe pour demander d'exécuter des ordres (en général, une transaction financière). La menace de cette pratique peut être croissante en raison des évolutions technologiques (cf. Deepfake[19]). Une variante consiste, pour le fraudeur, à se faire passer pour une administration de l'Etat dans le but d'obtenir des informations sur l'entreprise et ses clients ;
- **Tentatives de connexion** (41%), notamment par brute force[20] ;
- **Acquisition de noms de domaines illégitimes** (35%) ;
- **Attaque en déni de service** (33%).

En ce qui concerne les **vulnérabilités**, l'enquête révèle que les principales causes des incidents de sécurité sont les suivants :

- **Shadow IT** (44%) : cela désigne l'utilisation de systèmes (logiciels, appareils, applications, etc.) sans l'approbation de la direction des systèmes d'information ;
- **Vulnérabilités résiduelles permanentes** (36%) ;
- **Cyberattaque opportuniste** (36%) ;
- **Négligence ou erreur de manipulation** (33%) ;
- **Exposition de données sur un système géré par prestataire** (29%) ;
- **Dommage collatéral via un fournisseur atteint par une cyberattaque** (25%) ;
- **Cyberattaque ciblée** (24%).

[16] Baromètre de la cybersécurité des entreprise (Février 2021) : https://www.cesin.fr/fonds-documentaire-6eme-edition-du-barometre-annuel-du-cesin.html
[17] 228 entreprises, dont 55% de Grandes entreprises et 22% du secteur financier et assuranciel.
[18] Spear phishing : tentative d'hameçonnage ciblée ayant recours à l'ingénierie sociale.
[19] Le Deepfake est une technique reposant sur l'intelligence artificielle qui consiste notamment à superposer, dans une vidéo, le visage et la voix d'une personne sur une autre personne.
[20] L'attaque par brute force consiste à essayer de trouver un mot de passe en testant, une à une, toutes les combinaisons possibles.

Cette analyse préliminaire nous a notamment permis, au besoin, d'orienter nos questions lors de nos rencontres avec les opérationnels (cf. paragraphe suivant).

3.1.3. Réalisation d'entretiens

La cartographie des risques est réalisée par le biais d'entretiens avec le management d'activités opérationnelles (service informatique, gestion, juridique, actuaires produits et souscripteurs, etc.).

Pour chacun des risques identifiés lors des entretiens, une évaluation (à dire d'expert) de la fréquence et de la sévérité a été demandée. Les échelles de mesures, pour l'ensemble des entretiens, a été la suivante.

Table d'évaluation de la Fréquence	
Probabilité d'occurrence	**Elément de mesure**
Peu probable *	Occurrence quasi nulle (< 2%) sur 1 an (ou « *moins d'1 fois tous les 50 ans* »)
Possible **	Occurrence possible mais peu probable (2% à 10%) sur 1 an (ou « *1 fois tous les 50 ans à 1 fois tous les 10 ans* »)
Probable ***	Occurrence plausible (10% à 50%) sur 1 an (ou « *1 fois tous les 10 ans à 1 fois tous les 2 ans* »)
Presque certaine ****	Occurrence très probable (> 50%) sur 1 an (ou « *plus d'1 fois tous les 2 ans* »)

Table d'évaluation de la Sévérité		
Impact	**Financier (Résultat)**	**Image / réputation ou encore réglementaire**
Mineur *	< 5% du résultat annuel de EIG France	Attention de tiers (presse, groupes de pression, etc.) sur des sujets jugés sensibles
Modéré **	5% à 20% du résultat annuel	Communication défavorable dans des médias sur une partie de l'entreprise et à un niveau local
Majeur ***	20% à 50% du résultat annuel	Couverture médiatique plus large, mais n'entraînant pas d'effet majeur
Très significatif ****	> 50% du résultat annuel	Attaque médiatique ayant des conséquences significatives sur l'image et la réputation du Groupe

3.2. Identification et évaluation des risques

Nous présentons ici la cartographie établie à la suite des entretiens. **Le détail des risques identifiés se trouve en annexe 6.4**. Leur évaluation, basée sur jugements d'experts, a été réalisée compte tenu de leur probabilité d'occurrence et de leur impact sur EIG France. Il est à noter que, étant établie « à dire d'experts », cette cartographie peut nécessairement induire un biais.

Avertissement

Compte tenu de la sensibilité du sujet, il était délicat de présenter une évaluation réelle relative à la sécurité informatique d'une entreprise.
Néanmoins, dans le but de présenter un résultat cohérent et objectif, notre démarche a été la suivante :

- *Pour chacun des risques identifiés, nous avons chacun, de manière indépendante, évalué la probabilité d'occurrence et la sévérité.*
- *Nous avons ensuite confronté nos visions.*
- *Pour juger de la pertinence de notre évaluation (fictive), nous nous sommes rapprochés de personnes expérimentées sur le sujet. L'objectif étant de s'assurer que notre évaluation corresponde à l'état dans lequel pourrait se trouver une entreprise « moyenne ».*

				Risque brut[21]	
Identifiant du risque	**Famille de risque**	**Sous-famille de risque**	**Risque**	**Probabilité d'occurrence**	**Impact**
FI1	**Fraude interne**	Activité non autorisée	Modification des garanties des contrats	**	*
FI2			Modification des limites de délégation (souscription)	**	*
FI3		Vol et fraude interne	Divulgation de données financières	**	**
FI4			Accès à des informations à des fins de transactions financières (délit d'initié)	**	*
FI5			Diffusion d'informations stratégiques à l'extérieur	**	***
FI6			Paiement de fausses commissions	**	*
FI7			Paiement de faux sinistres	**	*
FI8			Dissimulation de fraude	**	*
FI9			Changement de bénéficiaires dans les systèmes	*	*
FI10		Sécurité des systèmes	Vol de données	***	***
FI11			Cryptage des données (ransomware)	*	***

[21] Pour faciliter la lecture dans la suite du rapport, nous précisons ici la différence que nous ferons entre « risque brut » et « risque net » :

- « risque brut » : risque (tenant compte des mesures de protection existantes et) **brut** des mesures d'atténuation que nous proposerons par la suite (cf. section 4.2) ;
- « risque net » : risque **net** des mesures d'atténuation qui seront proposées.

FI12		(interne) – Dommages volontaires	Destruction de données	*	***
FI13			Altération de données informatiques (qualité des données)	**	**
FI14			Modification des outils (tarification, détection de fraude, etc.)	*	**
FE1	**Fraude externe**	Vol et fraude externe	Cyber espionnage économique	*	*
FE2			Cyberattaque sur nos clients (faux site internet)	**	**
FE3			Usurpation de comptes sur les réseaux sociaux	**	**
FE4		Sécurité des systèmes (externe) – Dommages volontaires	Vol de données	***	***
FE5			Cryptage des données (ransomware)	***	***
FE6			Destruction de données	***	***
FE7			Altération de données informatiques (qualité des données)	***	**
C1	**Clients, produits et pratiques commerciales**	Conformité, diffusion d'informations et devoir fiduciaire	Diffusion de données clients sensibles à l'extérieur	***	****
C2			Retard de paiements des sinistres	***	**
C3		Pratiques commerciales ou de marché incorrectes	Gestion d'une demande de rançon (ransomware)	***	***
C4			Non-conformité à la réglementation	**	***
C5		Activités de conseil	Absence de réponse aux clients	***	**
D1	**Dysfonctionnements de l'activité et des systèmes**	Défaillance du système interne	Interruption des systèmes informatiques (serveurs)	***	***
D2			Indisponibilité des outils (logiciels)	***	**
D3		Défaillance du système externe	Inaccessibilité du site internet de l'entreprise (DDoS)	***	**
D4			Piratage du site internet de l'entreprise	**	**
D5			Inaccessibilité des logiciels d'un prestataire (SaaS)	**	**
D6			Infection d'un outil informatique d'un prestataire	**	**
D7			Inaccessibilité du compte de l'entreprise sur un réseau social	***	**
D8			Blackout (attaque du réseau électrique et de télécommunication)	*	***
E1	**Exécution, livraison et gestion des processus**	Saisie, exécution et suivi des transactions	Non-publication d'état règlementaire	*	**
E2			Retard de paiements à un prestataire	**	**
E3			Retard de paiements des charges sociales et fiscales	**	**
E4			Retard de paiements des salaires des employés	*	***

3.3. Synthèse de l'évaluation des risques

Compte tenu des risques identifiés ci-dessus et de leur évaluation, et afin de les hiérarchiser, nous construisons la matrice de criticité (fréquence/impact) ci-dessous :

Impact	Peu probable *	Possible **	Probable ***	Presque certaine ****
Très significatif ****			**[C1]** Diffusion de données clients sensibles à l'extérieur	
Majeur ***	**[FI11]** Cryptage des données (ransomware) **[FI12]** Destruction de données **[D8]** Blackout (attaque du réseau électrique et de télécommunication) **[E4]** Retard de paiements des salaires des employés	**[FI5]** Diffusion d'informations stratégiques à l'extérieur **[C4]** Non-conformité à la réglementation	**[FI10]** Vol de données **[FE4]** Vol de données **[FE5]** Cryptage des données (ransomware) **[FE6]** Destruction de données **[C3]** Gestion d'une demande de rançon (ransomware) **[D1]** Interruption des systèmes informatiques (serveurs)	
Modéré **	**[FI14]** Modification des outils (tarification, détection de fraude, etc.) **[E1]** Non-publication d'état règlementaire	**[FI3]** Divulgation de données financières **[FI13]** Altération de données informatiques (qualité des données) **[FE2]** Cyberattaque sur nos clients (faux site internet) **[FE3]** Usurpation de comptes sur les réseaux sociaux **[D4]** Piratage du site internet de l'entreprise **[D5]** Inaccessibilité des logiciels d'un prestataire (SaaS) **[D6]** Infection d'un outil informatique d'un prestataire **[E2]** Retard de paiements à un prestataire **[E3]** Retard de paiements des charges sociales et fiscales	**[FE7]** Altération de données informatiques (qualité des données) **[C2]** Retard de paiements des sinistres **[C5]** Absence de réponse aux clients **[D2]** Indisponibilité des outils (logiciels) **[D3]** Inaccessibilité du site internet de l'entreprise (DDoS) **[D7]** Inaccessibilité du compte de l'entreprise sur un réseau social	
Mineur *	**[FI9]** Changement de bénéficiaires dans les systèmes **[FE1]** Cyber espionnage économique	**[FI1]** Modification des garanties des contrats **[FI2]** Modification des limites de délégation (souscription) **[FI4]** Accès à des informations à des fins de transactions financières (délit d'initié) **[FI6]** Paiement de fausses commissions **[FI7]** Paiement de faux sinistres **[FI8]** Dissimulation de fraude		
	Probabilité d'occurrence			

4. Traitement des risques

4.1. Stratégie de gestion et priorisation des risques

La priorisation des risques est faite en lien avec la stratégie de gestion des risques de EIG France. C'est une traduction de ses objectifs stratégiques en un cadre de prise de risques. Cette stratégie de gestion des risques a pour but de garantir la maitrise de l'ensemble de ses risques aux niveaux individuel et agrégé.

La cartographie que nous avons établie a permis d'identifier 38 risques. Elle a été présentée au comité des risques opérationnels. Sur l'ensemble des risques identifiés et compte tenu de leur évaluation, le Directeur Général a demandé, lors de ce comité, de prioriser sept risques (précisés ci-après). Ces derniers sont classés comme « élevés » dans la cartographie et présentent un réel danger pour la stratégie de développement de EIG France.

La priorisation des risques étant faite, il est ensuite question de définir les stratégies de gestion de risque à appliquer parmi les suivantes :

- L'**acceptation** : le risque est accepté soit lorsque celui-ci entre dans la politique de gestion des risques de l'organisation, soit lorsque les coûts de mises en œuvre des éléments de maîtrise deviennent trop excessifs au regard du risque encouru ;
- La **réduction** : il s'agit de déployer des contrôles de sécurité et d'autres mesures pour réduire la probabilité et/ou l'impact et donc le niveau de risque ;
- Le **transfert** : cela consiste à partager une partie du risque avec d'autres parties par le biais de la cyber assurance ;
- Le **refus** : si le risque l'emporte sur les avantages, l'arrêt d'une activité peut être le meilleur plan d'action si cela signifie ne plus y être exposés.

Les stratégies retenues sont indiquées dans le tableau ci-dessous :

Identifiant du risque	Description du risque	Stratégie de gestion de risques
FI10	Vol de données *(Famille de risque : Fraude interne)*	REDUCTION
FE4	Vol de données *(Famille de risque : Fraude externe)*	REDUCTION TRANSFERT
FE5	Cryptage des données (ransomware)	
FE6	Destruction de données	
C1	Diffusion de données clients sensibles à l'extérieur	REDUCTION TRANSFERT
C3	Gestion d'une demande de rançon (ransomware)	TRANSFERT
D1	Interruption des systèmes informatiques (serveurs)	REDUCTION TRANSFERT

Nous nous sommes donc focalisés sur les mesures d'atténuation à appliquer sur ces risques. Compte tenu de l'interdépendance des risques identifiés dans la cartographie, le traitement de ces risques pourra également avoir un impact sur les autres risques.

Ces mesures d'atténuation sont détaillées dans la partie suivante.

4.2. Mesures d'atténuation

Les mesures d'atténuation présentées dans le tableau ci-dessous sont complémentaires à celles déjà en place. Ces mesures sont définies avec le Corporate Center et s'appuient sur les standards du Groupe EIG en matière de cybersécurité. Elles ont été validées au comité des risques opérationnels de EIG France et sont en cours d'implémentation.

Le détail, risque par risque, de l'impact des mesures d'atténuation pour l'ensemble des risques de la cartographie, **est disponible en annexe 6.5**.

		Risque brut*			Risque net*	
Identifiant du risque	**Description du risque**	**Occurrence**	**Impact**	**Atténuation du risque**	**Occurrence**	**Impact**
FI10	Vol de données	***	***	**[M1]** Poursuivre la sensibilisation des collaborateurs au risque Cyber **[M2]** Renforcer la sécurité des données sensibles **[M3]** Améliorer la sauvegarde **[M4]** Verrouiller l'écosystème informatique **[M5]** Renforcer la protection du SI contre les intrusions **[M6]** Réduire les comportements de contournement des règles sécuritaires **[M7]** Détecter et prévenir les comportements malveillants **[M8]** Réduire les risques relatifs à la sous-traitance **[M9]** Souscrire une assurance cyber risque	**	***
FE4	Vol de données	***	***		**	***
FE5	Cryptage des données (ransomware)	***	***		**	**
FE6	Destruction de données	***	***		**	**
C1	Diffusion de données clients sensibles à l'extérieur	***	****		**	***
C3	Gestion d'une demande de rançon (ransomware)	***	***		**	**
D1	Interruption des systèmes informatiques (serveurs)	***	***		**	**

** : Comme indiqué en section 3.2 (cf. note de bas de page), pour faciliter la lecture, nous précisons ici la différence que nous faisons entre « risque brut » et « risque net » :*

- *« risque brut » : risque (tenant compte des mesures de protection existantes et) **brut** des mesures d'atténuation que nous proposons ;*
- *« risque net » : risque **net** des mesures d'atténuation proposées.*

4.2.1. [M1] Poursuivre la sensibilisation des collaborateurs au risque Cyber

L'humain reste un facteur clé dans la lutte contre le risque Cyber car il est le premier rempart face à ce risque. Les collaborateurs de EIG France doivent continuer à être sensibilisés aux risques de cybersécurité, notamment avec des mails de communication appelant à la vigilance, en rappelant régulièrement les dix règles de base de l'ANSSI[22], des e-learnings et des campagnes de phishing permettant d'acquérir les bons réflexes. De même, les prestataires doivent être sensibilisés à ces risques pour ne pas représenter le maillon faible de la protection face aux cybermenaces.

La mise en place d'un Groupe de Travail « Sécurité Informatique », regroupant des représentants de toutes les directions, peut être une bonne pratique à appliquer pour EIG France. L'objectif serait, pour les représentants, de faire redescendre l'information et sensibiliser les autres collaborateurs.

4.2.2. [M2] Renforcer la sécurité les données sensibles

La **classification[23] des données** joue un rôle important dans leur sécurité. En effet, elle garantit l'identification et la catégorisation des données sensibles afin que celles-ci reçoivent le niveau de protection approprié. Il s'est avéré, à l'occasion des entretiens, que le processus de classification des données n'était pas suffisamment bien établi au sein de EIG France.

De plus, pour renforcer la sécurité des données sensibles, il est recommandé de :

- Introduire un **mécanisme de détection et d'alerte de fuites de données** telle que les sondes de détection et de surveillance OSINT[24] ;
- Limiter le nombre d'utilisateurs avec les profils applicatifs les plus sensibles (accès aux données médicales, gestion d'actifs, etc.) par la mise en place des profils métier dans le cadre du processus IAM[25].

Le **niveau de sécurité des fournisseurs et des partenaires** doit être évalué lorsque des données sont confiées à l'extérieur.

4.2.3. [M3] Améliorer la sauvegarde

La sauvegarde actuelle des données doit être renforcée avec une **sauvegarde offline** (i.e. non connectée à un réseau) ou externalisée. De plus, bien que le processus de sauvegarde actuel soit quotidien, il est nécessaire de réaliser de **tests réguliers de la capacité de récupération** des sauvegardes.

---

[22] https://www.ssi.gouv.fr/administration/precautions-elementaires/10-regles-de-base/

[23] La classification des données est un processus de catégorisation cohérente des données sur la base de critères spécifiques et prédéfinis, afin qu'elles puissent être utilisées et protégées efficacement.

[24] Open Source Intelligent (OSINT) fait référence à la collecte d'informations auprès des sources publiques pour les utiliser dans le contexte du renseignement.

[25] L'Identity and Access Management (IAM) est un ensemble de processus mis en place par la Direction des Systèmes d'Information pour la gestion des habilitations des utilisateurs (qui peuvent être des collaborateurs, des prestataires, des intérimaires, etc.) afin de réglementer l'accès au réseau et aux applications Cloud.

4.2.4. [M4] Verrouiller l'écosystème informatique

Afin de lutter contre les fuites de données de façon générale, le verrouillage complet de l'écosystème informatique mis en place au niveau du Corporate Center doit être déployé au sein de EIG France. Ainsi, les **ports USB des ordinateurs doivent être fermés** en écriture, **le transfert de données en externe** (sites internet, e-mails, etc.) et **l'impression doivent être contrôlés.**

4.2.5. [M5] Renforcer la protection du SI contre les intrusions

Pour consolider la protection du SI contre des intrusions, le dispositif actuel peut être complété par :

- des outils de **surveillance de type IPS** (« Intrusion Protection System ») qui filtrent les entrées et les sorties pour détecter et écarter un certain nombre d'intrusions malveillantes ;
- des **scanners de vulnérabilité** qui permettent l'identification de vulnérabilités sur les composants du Système d'Information par une approche active via des outils automatisés. Cette identification permet de corriger les failles, avant qu'elles ne soient exploitées par une menace.

Cela permettra ainsi de déceler les intrusions dans le SI.

Les nouvelles applications exposées et/ou sensibles doivent faire l'objet de **tests de pénétration et de scans réguliers** afin d'identifier les vulnérabilités qui pourraient être exploitées par les attaquants. Pour cela, et de manière plus générale pour **identifier ses vulnérabilités résiduelles**, EIG France peut faire appel, à intervalle régulier, à des **sociétés de hackers éthiques**.

4.2.6. [M6] Réduire les comportements de contournement des règles sécuritaires

Au cours de notre mission nous avons identifié que, dans le cadre de son développement, EIG France avait mis en place de nombreux outils où la DSI était intégrée tardivement dans la conception du projet, voire pas intégrée (cas de « Shadow IT »). Pour lutter contre le Shadow IT, il est essentiel de communiquer davantage sur les bénéfices d'intégrer la DSI dans tous les projets développés en interne, dès leur lancement. Cela passe par une approche « **Security by design** » des solutions développées. Cela permettra ainsi, outre un gain de temps dans le déploiement d'outils, de veiller au maximum au respect des règles sécuritaires.

4.2.7. [M7] Détecter et prévenir les comportements malveillants

Les cas de comportements malveillants peuvent traduire un sentiment de colère (injustice, frustration, etc.) d'un collaborateur. Pour limiter ces cas, un climat et un leadership exemplaire, juste et éthique est nécessaire. La **mise en place d'enquêtes de satisfaction** internes régulières auprès de l'ensemble des collaborateurs de EIG France peut contribuer à (i) détecter des environnements à risque et (ii) renforcer la satisfaction au travail, dans le but de prévenir des comportements à risque.

4.2.8. [M8] Réduire les risques relatifs à la sous-traitance

EIG France doit exiger de ses sous-traitants un niveau de sécurité proportionné à la sensibilité des données transmises et le matérialiser contractuellement. Le contrat de sous-traitance doit comporter des éléments de prévention du risque Cyber, et EIG France doit disposer d'une capacité de contrôle de ses prestataires de service (audit).

4.2.9. [M9] Souscrire une assurance cyber risque

Pour l'accompagner dans la gestion de crise et limiter les impacts des risques identifiés, tant en termes financier qu'en termes d'image, EIG France peut souscrire une assurance cyber risque couvrant en particulier :

- les coûts résultant de l'attaque : expertise judiciaire, conseils juridiques, notification des clients / organismes règlementaires, surveillance du crédit des clients concernés ;
- les dommages : réparation, restauration ou remplacement si un hacker cause des dommages au site internet, aux programmes ou aux données électroniques ;
- les ransomwares ;
- l'interruption d'activité sans dommages : vérifier que la couverture actuelle de EIG France s'applique bien au cas de risque informatique.

Il est à noter que la mise en place des mesures d'atténuation listées ci-avant permettra de réduire le coût de la couverture (i.e. la prime d'assurance).

4.3. Synthèse de l'évaluation des risques nets des mesures d'atténuation

Nous établissons ci-dessous la classification des risques nets des mesures d'atténuation retenues :

Impact					
	Très significatif ****				
	Majeur ***	**[D8]** Blackout (attaque du réseau électrique et de télécommunication) **[E4]** Retard de paiements des salaires des employés	**[FI5]** Diffusion d'informations stratégiques à l'extérieur **[FI10]** Vol de données **[FE4]** Vol de données **[C1]** Diffusion de données clients sensibles à l'extérieur		
	Modéré **	**[FI11]** Cryptage des données (ransomware) **[FI12]** Destruction de données **[FI14]** Modification des outils (tarification, détection de fraude, etc.) **[FE3]** Usurpation de comptes sur les réseaux sociaux **[E1]** Non-publication d'état règlementaire	**[FI3]** Divulgation de données financières **[FI13]** Altération de données informatiques (qualité des données) **[FE2]** Cyberattaque sur nos clients (faux site internet) **[FE5]** Cryptage des données (ransomware) **[FE6]** Destruction de données **[FE7]** Altération de données informatiques (qualité des données) **[C3]** Gestion d'une demande de rançon (ransomware) **[C4]** Non-conformité à la réglementation **[D1]** Interruption des systèmes informatiques (serveurs) **[D2]** Indisponibilité des outils (logiciels) **[D4]** Piratage du site internet de l'entreprise **[D5]** Inaccessibilité des logiciels d'un prestataire (SaaS) **[D6]** Infection d'un outil informatique d'un prestataire **[D7]** Inaccessibilité du compte de l'entreprise sur un réseau social **[E2]** Retard de paiements à un prestataire **[E3]** Retard de paiements des charges sociales et fiscales	**[C2]** Retard de paiements des sinistres **[C5]** Absence de réponse aux clients **[D3]** Inaccessibilité du site internet de l'entreprise (DDoS)	
	Mineur *	**[FI9]** Changement de bénéficiaires dans les systèmes **[FE1]** Cyber espionnage économique	**[FI1]** Modification des garanties des contrats **[FI2]** Modification des limites de délégation (souscription) **[FI4]** Accès à des informations à des fins de transactions financières (délit d'initié) **[FI6]** Paiement de fausses commissions **[FI7]** Paiement de faux sinistres **[FI8]** Dissimulation de fraude		
		Peu probable *	*Possible* **	*Probable* ***	*Presque certaine* ****
		Probabilité d'occurrence			

4.4. Mise en place de KRI complémentaires

Les KRI (Key Risk Indicators) ont pour objectif de fournir une évaluation régulière des améliorations ou détériorations du profil de risque ou de l'environnement de prévention et de contrôle. En complément des KRI existants, de nouveaux indicateurs (cf. tableau ci-dessous) ont été proposés et validés en comité des risques opérationnels. Leur mise en place permettra un meilleur contrôle du risque Cyber au sein de EIG France.

Risque	Indicateur	Responsable
Fuite de données sensibles à fort impact	Nombre de fuites de données classées « Confidentielles » avec un impact significatif	RSSI
	Nombre de fuites de données client sensibles (au sens de la règlementation RGPD) ayant entrainé une notification au régulateur	RSSI
	% de comptes avec ports USB ouverts	RSSI
	% de comptes avec droit administrateur	RSSI
Défaillance de services à fort impact	% d'applications critiques avec obsolescence	RSSI
Défaillance système (externe)	Nombre de cyberattaques sur un fournisseur/sous-traitant ayant entrainé (i) un coût supérieur à 1 M€, (ii) une destruction, (iii) une modification ou (iv) un vol de données de EIG France	Responsable des opérations
Facteur humain	% de personnes ayant cliqué sur le lien lors des campagnes de phishing	RSSI
	% de personnes ayant validé la formation de cyber sécurité dans les 12 derniers mois	DRH
Perte ou dégradation de données	Nombre de violations IT ayant des conséquences matérielles sur les données (perte, compromission)	RSSI
DDoS	Nombre de connexions internet suspectes* par jour	RSSI

**Connexions « suspectes » : ne correspondant pas à la politique d'accès à internet définie par EIG France (ex. : sites illégaux ou considérés dangereux, publicité bloquée dans les pages web, etc.).*

5. Conclusion

Avec la digitalisation massive de notre société, le **risque Cyber est aujourd'hui considéré comme l'un des principaux risques** auxquels les citoyens et entreprises sont confrontés. Les entreprises des secteurs financier et assuranciel sont non seulement des cibles de choix pour les pirates informatiques, mais elles doivent, dans le même temps, **accélérer sur la digitalisation**. Un mouvement rendu inévitable à la fois par le développement de nouveaux usages digitaux (accéléré par la pandémie de Covid-19) ainsi que par l'émergence de nouveaux acteurs comme les « fintechs » ou les « insurtechs ».

L'objectif de ce rapport était de déployer une démarche ERM, appliquée à la gestion du risque Cyber de EIG France, dans le but d'aider l'entreprise à **maîtriser ce risque** pour poursuivre sereinement sa nécessaire transformation digitale.

La cartographie des risques alors établie a permis d'**identifier** les principaux risques auxquels l'entreprise est exposée. Leur **évaluation**, tenant compte de leurs fréquence et impact potentiel, permet de mettre en avant les risques les plus significatifs pour EIG France. D'évidence, il n'est pas possible de traiter tous les risques relevés ; d'où l'importance de les prioriser compte tenu des objectifs stratégiques de EIG France. Sept risques ont ainsi été **priorisés et traités**, par la définition de stratégies de gestion et l'application de mesures d'atténuation. Nous notons par ailleurs que le traitement de ces sept risques priorisés, qui renforce l'**environnement de contrôles**, permet également de réduire les autres risques ; ce qui met en exergue l'interdépendance des risques.

Ainsi, il est important pour une entreprise d'assurance de cadrer sa politique de défense contre le risque Cyber avec des **méthodes**, une **organisation** et une **gouvernance** adaptées. Si la **maîtrise technique** est de toute évidence indispensable, l'**humain** reste un facteur clé dans la lutte contre le risque Cyber car il en est le premier rempart.

Toutefois, malgré les dispositifs de protection en place, les cyberattaques semblent inéluctables car le risque n'est pas figé : les hackers possèdent une technicité qui évolue et, si l'on peut espérer que l'industrie informatique améliore progressivement la sécurité, le modèle économique de la sécurité informatique induit nécessairement une croissance du nombre de failles exploitables[26]. EIG France doit donc procéder à des **évaluations régulières** de ses procédures pour réduire les impacts au maximum mais aussi développer ses **capacités de résilience** et de **continuité d'activité** face à ce risque incontournable.

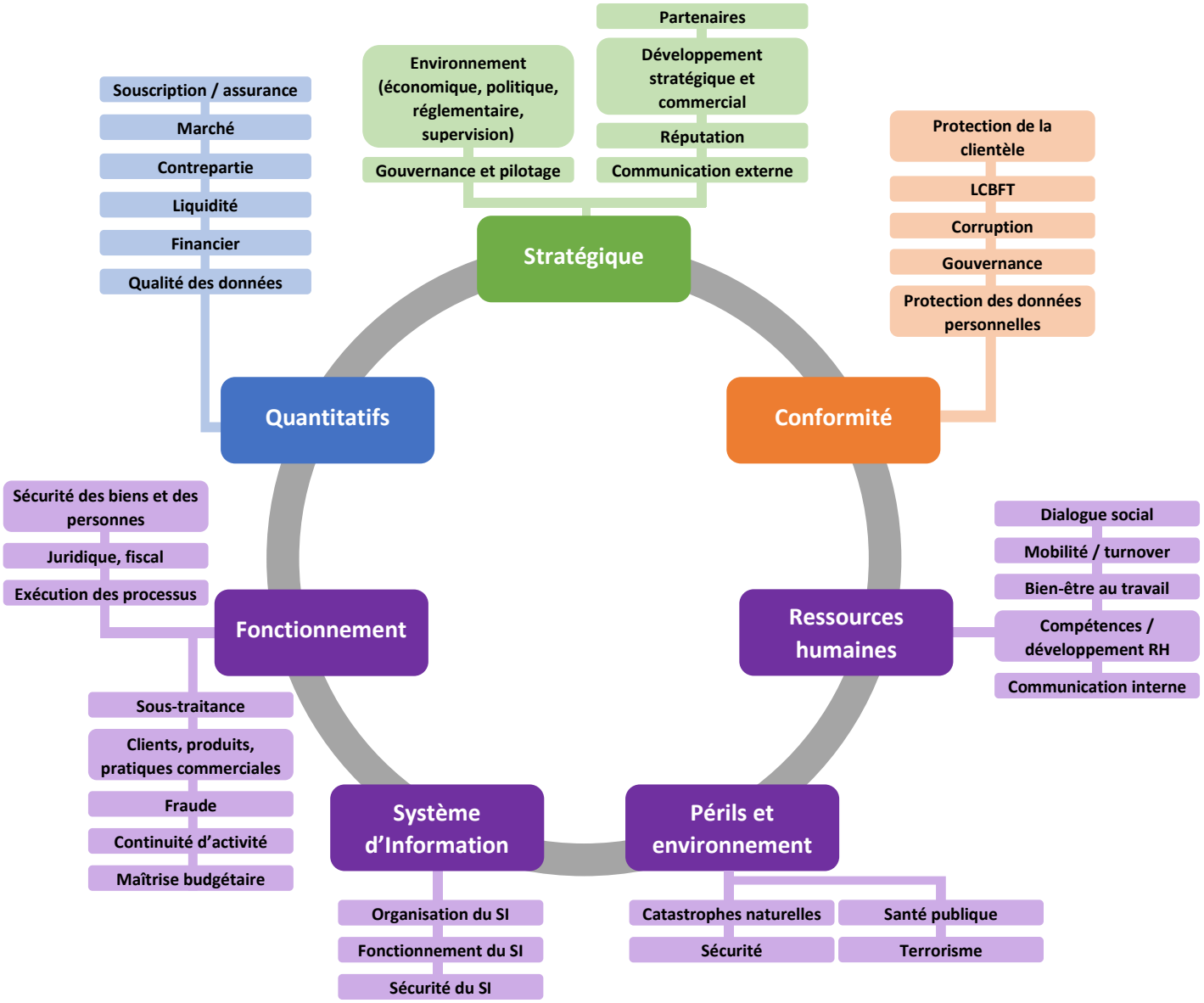
Ce rapport, à travers les cas exposés, traite en filigrane les menaces émanant de hackers isolés ou d'organisations criminelles, pour lesquelles les moyens (i.e. le budget) sont plus ou moins importants, mais tout de même limités. Ce qui est cohérent avec le dimensionnement de EIG en France : bien qu'important, EIG n'est pas encore l'acteur majeur sur le marché français. Si toutefois elle était amenée à le devenir, le recours à la prospective pourrait être intéressant pour venir compléter l'analyse de ce sujet. En effet, les tensions aujourd'hui dans le cyberespace sont telles que l'on s'interroge sur « **l'existence d'une Guerre froide dans le cyberespace** »[27]. Un assureur de taille significative, acteur majeur de l'économie à l'échelle nationale (épargne de la population, financement et investissements dans des entreprises ou la Recherche, etc.), pourrait représenter une **cible stratégique** pour un acteur étatique, de « budget d'attaque » illimité, souhaitant **déstabiliser l'économie d'une puissance**.

[26] Des chercheurs ont identifié plusieurs caractéristiques des marchés de services et produits numériques qui favorisent le temps de mise sur marché au détriment de la sécurité (R. Anderson and T. Moore, "Information Security Economics – and Beyond" - https://link.springer.com/chapter/10.1007/978-3-540-74143-5_5).

[27] Comme l'a ainsi déclaré la ministre des Armées Florence Parly au Forum International sur la Cybersécurité (septembre 2021).

6. Annexes

6.1. Nomenclature des risques de EIG France[28]



[28] Référence (repris pour exemple) : « Transformation digitale et évolution du profil de risque : mise en œuvre d'un cadre ERM » (J. DEJONGHE, 2019)

6.2. Définition des familles et sous-familles de risque Cyber[29]

Famille	Sous-famille
Fraude interne Le risque de fraude interne est le risque résultant d'un abus délibéré des procédures, des systèmes, des actifs, des produits et/ou des services d'une entreprise impliquant au moins un membre du personnel interne qui a l'intention de tromper ou de profiter illégalement à lui-même ou à d'autres.	**Activité non autorisée** Manquements à l'autorité qui ne sont pas des activités criminelles. C'est-à-dire que l'employé peut être licencié mais pas poursuivi. Cela comprend le risque de perte causée par des activités d'employés non autorisées, des approbations ou un dépassement de l'autorité.
	Vol et fraude interne L'activité est de nature criminelle et entraînerait des poursuites. Inclut le risque de détournement d'actifs, de fraude collusoire et de corruption et le risque de fraude à l'information financière.
	Sécurité des systèmes (interne) – Dommages volontaires Inclut le risque de perte financière due à des activités non détectées telles que des modifications non autorisées des paramètres de sécurité clés, des tentatives infructueuses répétées de se connecter à un système sensible et l'insertion de logiciels malveillants.
Fraude externe Evénements résultant d'actes de fraude et de vols, ou de contournement intentionnel de la loi, commis par des tiers, y compris des clients, des vendeurs et des sociétés sous-traitantes, dans le but d'obtenir un avantage personnel, portant préjudice à la Société ou à ses contreparties (pour lesquelles la Société paie), ou endommager les actifs de la Société. Cela comprend les fraudes par les clients et les parties externes (c'est-à-dire les parties qui ne collaborent généralement pas avec la Société et n'ont pas accès	**Vol et fraude externe** Vol/Vol d'actifs corporels et incorporels par des tiers (sans violation du système de l'entreprise). Fraude par des tiers, y compris des clients, des fournisseurs et des sociétés d'externalisation, dans le but d'obtenir un avantage économique personnel et de causer des dommages à la Société. Cela ne comprend pas : a) collusion avec un membre du personnel qui est considérée comme une fraude interne b) Fraude liée au système qui est classée comme EL0202
	Sécurité des systèmes (externe) – Dommages volontaires

[29] Traduction de la catégorisation issue du document « Supporting on-going capture and sharing of digital event data » (CRO Forum 2018)

Famille	Sous-famille
aux systèmes de la Société, tels que les courtiers non mécanisés).	Piratage ou tentative d'accès aux systèmes de la Société à des fins de vol, d'utilisation et de manipulation inappropriées d'informations ou pour voler ou endommager des données sur les systèmes.
Clients, produits et pratiques commerciales Manquements involontaires ou négligence (imprudence) à remplir une obligation professionnelle envers des clients spécifiques (y compris les exigences fiduciaires et de conformité) et les parties prenantes de l'entreprise, par ex. régulateurs, ou de la nature ou de la conception d'un produit.	**Conformité, diffusion d'informations et devoir fiduciaire** La sous-catégorie de conformité, de diffusion d'informations et d'obligation fiduciaire couvre les événements de risque opérationnel résultant d'infractions ou de défaillances réglementaires ayant un impact sur les clients, les clients ou les partenaires commerciaux.
	Pratiques commerciales ou de marché incorrectes La sous-catégorie des pratiques commerciales ou de marché incorrectes couvre les événements de risque opérationnel résultant de pratiques commerciales incorrectes présumées.
	Activités de conseil La sous-catégorie des activités de conseil doit être utilisée lorsqu'un événement de risque opérationnel survient en raison d'un manquement aux obligations.
Dysfonctionnements de l'activité et des systèmes Evénements de perte associés à l'interruption de l'activité commerciale en raison de défaillances internes ou externes du système et/ou du système de communication, de l'inaccessibilité des informations et/ou de l'indisponibilité des services publics et d'autres perturbations commerciales externes qui peuvent également nuire au personnel.	**Défaillance du système interne** Les événements de perte associés à l'interruption de l'activité commerciale en raison d'un dysfonctionnement du système interne, d'un dysfonctionnement ou d'une panne de l'EUC et/ou de défaillances du système de communication interne et/ou de l'inaccessibilité des informations et/ou de la perte de données. Une filiale à 100 % gérant l'informatique est considérée comme interne.
	Défaillance du système externe Les événements de perte associés à l'interruption de l'activité commerciale en raison d'un système externe, de défaillances de fournisseurs informatiques externes et/ou de défaillances du système de communication externe et/ou de l'indisponibilité des services publics.

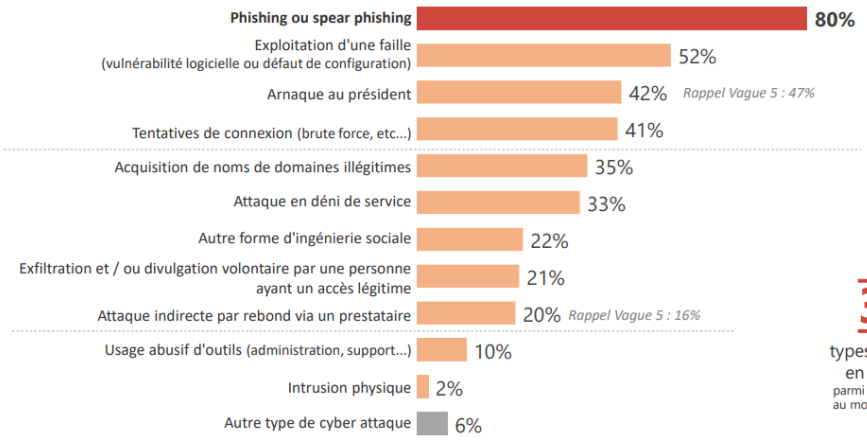
Famille	Sous-famille
Exécution, livraison et gestion des processus Pertes résultant de l'échec du traitement des transactions ou de la gestion des processus, des relations avec les contreparties commerciales et les fournisseurs.	**Saisie, exécution et suivi des transactions**

6.3. Vecteurs et causes de cyberattaques en entreprises en France

Extrait du Baromètre de la cybersécurité des entreprises (CESIN, Février 2021)[30]

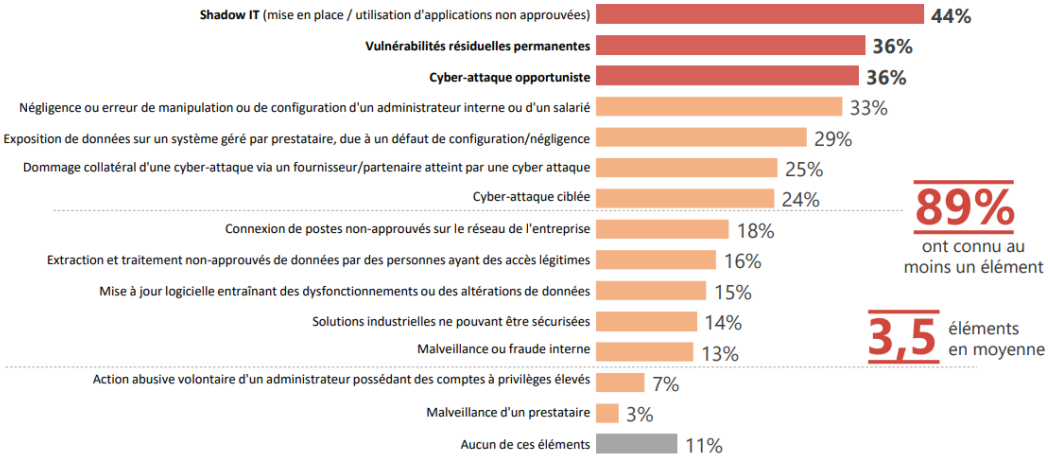
Le phishing, premier vecteur d'attaque dans les entreprises

Q5A. Parmi les vecteurs d'attaques suivants, lesquels ont impacté votre entreprise au cours des 12 derniers mois ?
Base : ont constaté une attaque (129) / Plusieurs réponses possibles



Le Shadow IT est la principale cause des incidents de sécurité rencontrés par les entreprises

Q6. Parmi les causes des incidents de sécurité rencontrées par l'entreprise, cyber-attaques incluses, quelles sont celles auxquelles votre entreprise a été concrètement confrontée au cours des 12 derniers mois ?
Base : ensemble (228) / Plusieurs réponses possibles



[30] https://www.cesin.fr/fonds-documentaire-6eme-edition-du-barometre-annuel-du-cesin.html

6.4. Détail des risques identifiés pour EIG France

6.4.1. Fraude interne

Nous identifions, dans cette catégorie, les risques de fraude impliquant au moins une personne interne à EIG France et agissant de manière délibérée, que cela soit dans son unique intérêt ou non. La fraude peut être relative à :

- une **activité non autorisée** : une prise d'engagement en l'absence d'autorisation (i.e. dépassement des limites autorisées) ;
- un **vol ou une fraude interne** : un acte frauduleux résultant de manipulations de données internes ;
- la **sécurité des systèmes et dommages volontaires** : des activités affectant les systèmes de EIG France.

❖ *Activité non autorisée*

Pour ce qui concerne les risques relatifs à des activités non autorisées, ceux-ci peuvent être relatifs à la gestion des contrats. En effet, un gestionnaire de EIG France, qui a accès aux caractéristiques des contrats, pourrait **modifier les garanties d'un contrat** (risque référencé « **FI1** » dans la cartographie des risques, cf. section 3.2).

En outre, la politique de souscription de EIG France définit le cadre et les limites dans lesquelles un souscripteur peut agir dans la souscription d'une affaire. Certaines autorisations sont ainsi accordées à des collaborateurs qualifiés. Ces autorisations sont documentées et intégrées dans l'outil de gestion. Si une **modification des limites autorisées est effectuée dans le système informatique** (**FI2**), le gestionnaire peut être amené à prendre des positions non autorisées.

❖ *Vol et fraude interne*

Les données financières de EIG France représentent des informations sensibles. En effet, elles peuvent donner des informations sur l'état de santé de l'entreprise. Certains collaborateurs disposent d'un accès à des informations sensibles sur l'entreprise (ratio de solvabilité prévu, éventuelles pertes conséquentes que l'entreprise peut subir, etc.) et la **divulgation de ces données financières** (**FI3**) peut être préjudiciable pour EIG. En effet, cela peut entrainer des mouvements sur les marchés qui pourraient perturber la stabilité de l'entreprise. De même, un risque peut être qu'une **personne non autorisée accède à ce type d'informations dans le but d'effectuer des transactions financières** (**FI4**) ; il s'agirait alors d'un délit d'initié.

Par ailleurs, certains collaborateurs ont accès à des données stratégiques (fusion ou acquisition d'entreprises envisagées, signature de partenariat avec un acteur stratégique, éventuelles cessions de certaines activités, etc.). Le besoin de respecter la confidentialité de ces informations est d'autant plus important qu'une **fuite de ces données stratégiques** (**FI5**) pourrait compromettre la bonne application de la stratégie que EIG France a envisagé d'appliquer.

Dans les activités les plus communes, il y a notamment le paiement des factures ou commissions à des apporteurs. Un risque identifié en termes de fraude interne est le **paiement de fausses commissions** (**FI6**), qui peuvent impacter les résultats de EIG France, de manière plus ou moins significative selon l'ampleur de la fraude.

En parallèle, il y a également le **paiement de faux sinistres** (**FI7**), pour lesquels la prime collectée n'est pas censée couvrir un sinistre « inexistant », ce qui peut déstabiliser l'équilibre technique. Il peut s'agir d'un paiement frauduleux à un vrai client (complicité) ou à un faux client (un gestionnaire réaliserait un versement de prestations pour son compte).

Par ailleurs, la complicité d'un collaborateur interne de EIG France avec un client fraudeur de l'Enterprise, peut amener à **dissimuler une fraude** (**FI8**) en faussant les moyens de détection.

Enfin, toujours sur le registre des paiements, une fraude qui pourrait être observée serait le **changement de bénéficiaires dans le système de gestion** (**FI9**) : un gestionnaire renseignerait un compte bancaire lui permettant, par des moyens détournés, de bénéficier du règlement qui aurait dû être versé à un vrai client sinistré.

- *Sécurité des systèmes (interne) – Dommages volontaires*

Nous identifions ici les activités qui affectent les systèmes internes de l'entreprise, comme le **vol de données** (**FI10**) : un employé va s'approprier ou aider à s'approprier des données spécifiques de EIG France, notamment des informations clients sensibles, comme les noms, prénoms, date de naissance, mais également les questionnaires de santé, données financières de nos clients, etc. La vente de données personnelles est une activité majeure dans le cyberespace criminel. En effet, un rapport de l'ANSSI[31], met en évidence que les données personnelles (adresse mail, profession, numéro de sécurité sociale, etc.) servent à mener des opérations de fraudes (usurpation d'identité, fraudes aux aides sociales, etc.). Les cybercriminels peuvent également s'en servir dans des manœuvres d'ingénierie sociale[32]. L'hameçonnage ciblé, qui est un des vecteurs d'infection majeurs, s'appuie sur ce genre de données afin de personnaliser le contenu des mails malveillants et inciter les cibles à les ouvrir.

Un autre risque identifié est le **cryptage de données dû à un ransomware** (**FI11**) : les données de l'entreprise sont rendues inexploitables par des logiciels de cryptage. Généralement, s'en suit une demande de rançon, proposant la clé de décryptage en échange de transaction financière. On parle alors de rançongiciel (« *ransomware* » en anglais). Le risque pour EIG France est la mise à l'arrêt résultant de ce cryptage de données. En effet, si les données ne sont plus exploitables, cela peut endommager la bonne conduite des activités, voire les paralyser. Il s'agit d'un risque qui se démocratise dans le cyber espace, via notamment le « *Ransomware-As-A-Service* »[33] : des groupes criminels proposent leurs codes malveillants à la location.

Au-delà du cryptage, la **destruction des données** (**FI12**) peut également porter préjudice à EIG France. Un employé, s'apprêtant à quitter l'entreprise dans de mauvaises circonstances, pourrait décider, par rancœur, de supprimer certaines informations importantes relatives ou non à son activité.

En outre, un risque induit par les dommages portés aux systèmes est l'impact que cela a sur la qualité des données. En effet, une **altération des données informatiques** (**FI13**) peut impacter à la fois la gestion des contrats comme l'aspect technique (double paiement de facture, provisionnement inapproprié en cas de pertes partielles d'information, analyse technique biaisée, etc.).

[31] Etat de la menace rançongiciel (2020) : https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf
[32] L'ingénierie sociale est une pratique de manipulation psychologique (tromperie) à des fins d'escroquerie.
[33] *Ransomware-As-A-Service* (RaaS) fait l'analogie au « *Software-As-A-Service* » (SaaS), un modèle d'exploitation commerciale de logiciels, où les logiciels sont installés sur des serveurs distants plutôt que sur la machine de l'utilisateur et les clients paient un abonnement plutôt qu'une licence d'utilisation. Ce modèle est de plus en plus utilisé par les éditeurs (par exemple Microsoft, avec Office 365).

Enfin, au-delà des données, il y a également les outils : un employé pourrait décider de **modifier les outils** (**FI14**) tels que ceux utilisés, par exemple, pour la tarification, détection de fraudes, etc., qui sont aujourd'hui importants pour EIG France, et risqueraient ainsi de ne plus être efficients.

6.4.2. Fraude externe

Nous identifions, dans cette catégorie, les risques relatifs à des fraudes réalisées par des tiers. De manière analogue à la fraude interne, elle peut être relative à :

- un **vol ou une fraude externe** ;
- la **sécurité des systèmes et dommages volontaires**.

❖ *Vol et fraude externe*

Les actes de vol externe peuvent être relatifs à du **cyber espionnage économique** (**FE1**) : observer silencieusement les agissements internes de l'entreprise dans le but d'anticiper ses manœuvres.

Nos **clients peuvent également être la cible de cyberattaques** (**FE2**) via notamment la création d'un faux site internet, ressemblant à celui de EIG France, afin de capter leurs informations.

Enfin, nous identifions également le risque d'**usurpation de comptes sur les réseaux sociaux** (**FE3**) : si un tiers obtient l'accès au compte de EIG France sur un réseau social, de son Directeur Général ou d'une autre personne associée à la marque EIG, l'image de l'entreprise peut se retrouver écornée.

❖ *Sécurité des systèmes (externe) – Dommages volontaires*

Comme pour les risques de fraude interne, nous identifions ici le **vol de données** (**FE4**), le **cryptage des données (ransomware)** (**FE5**), la **destruction de données** (**FE6**) ou encore l'**altération des données informatiques** (**FE7**), réalisés dans le cadre d'un piratage, par des tiers.

Ces risques sont d'autant plus élevés pour EIG France, de taille significative, que la tendance dans la cybercriminalité est au « *Big Game Hunting* » : cibler les entreprises en fonction de leurs (fortes) capacités de paiement pour y déployer un ransomware.

6.4.3. Clients, produits et pratiques commerciales

Dans cette catégorie, nous identifions les risques relatifs à des manquements à une obligation professionnelle envers des clients ou des pratiques de marché incorrectes. Cela peut être relatif à :

- **Conformité, diffusion d'informations et devoir fiduciaire** : une défaillance ayant un impact sur le client ;
- **Pratiques commerciales ou de marché incorrectes** : des pratiques pouvant entrainer des sanctions financières ;
- **Activités de conseil** : une défaillance vis-à-vis du devoir de conseil auprès du client.

❖ *Conformité, diffusion d'informations et devoir fiduciaire*

Le client est d'évidence au centre des préoccupations de EIG, et la confiance qu'il a envers l'entreprise est clé dans notre fonctionnement. Une **diffusion de ses données** (**C1**) peut entrainer une perte de confiance et ainsi compromettre notre activité d'assureur.

En outre, une cyberattaque subie peut perturber le bon déroulement de nos activités et entrainer d'éventuels **retards de paiements des sinistres de nos clients** (**C2**), ce qui, là-aussi, peut écorner la relation client.

❖ *Pratiques commerciales ou de marché incorrectes*

Dans le cas d'une attaque au rançongiciel, le risque auquel EIG France est confrontée, au-delà de ceux relatifs aux données, est la **gestion d'une demande de rançon** (**C3**). Bien qu'actuellement, en France, le paiement d'une rançon ne soit pas interdit légalement, la situation pourrait potentiellement évoluer. En effet, il est, d'une part, évident que le paiement de rançons peut encourager la cybercriminalité. D'autre part, lors de discussions récentes au Sénat sur le sujet[34], il a été évoqué que le paiement de rançons contribuerait en quelque sorte au financement du terrorisme. Aux Etats-Unis, par exemple, les entreprises victimes de rançongiciel peuvent être sanctionnées par les autorités américaines en cas de paiement de rançons[35].

Par ailleurs, après une cyberattaque avérée, EIG France a des obligations réglementaires à respecter (communication aux autorités – ACPR, ANSSI, CNIL – aux clients, etc.). La responsabilité de l'entreprise pourrait être mise en cause pour **non-conformité à la réglementation** (**C4**) et entrainer des sanctions.

❖ *Activités de conseil*

Comme pour le cas des retards de paiements, en cas d'activité perturbée, EIG France pourrait se trouver dans une situation où elle n'est pas en mesure de répondre aux attentes de ses clients : des demandes clients pourraient se trouver en **absence de réponse** (**C5**).

6.4.4. Dysfonctionnements de l'activité et des systèmes

Nous identifions ici les dysfonctionnements de l'activité résultant d'une défaillance des systèmes. Nous distinguons :

- les **défaillances du système interne** : cela concerne le Système d'Information interne de EIG France ;
- les **défaillances du système externe** : cela concerne les parties externalisées (via prestataire, hébergeur, etc.).

[34] Table ronde « la cybersécurité des ETI-PME-TPE : la réponse des pouvoirs publics » (avril 2021) : http://www.senat.fr/compte-rendu-commissions/20210412/2020_04_15.html
[35] https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20201001

❖ *Défaillance du système interne*

Une cyberattaque sur le réseau informatique de EIG France peut amener à une **interruption de serveurs** (**D1**), volontaire (pour éviter une propagation d'un virus) ou involontaire (conséquence de l'attaque). Par la même occasion, certains **outils (logiciels) peuvent être rendus indisponibles** (**D2**).

❖ *Défaillance du système externe*

Dans le cadre de son écosystème informatique, EIG France fait appel à des prestataires (site internet, hébergeur Cloud, etc.). Les attaques subies par le prestataire peuvent ainsi avoir des conséquences pour l'entreprise.

Une attaque en déni de service[36] pourrait rendre le **site internet de EIG France inaccessible** (**D3**), ce qui peut entrainer une perte de productivité pour l'entreprise. Véritable vitrine de l'entreprise, le **site internet peut également être une cible de choix pour un piratage** (**D4**) dans le but d'obtenir des données clients.

De même, EIG France utilise des logiciels hébergés en Cloud (cf. *Software-As-A-Service*) ; son activité dépend donc de la bonne sécurisation de ceux-ci : l'**inaccessibilité de ces logiciels** (**D5**), faisant suite à une attaque ciblée sur un prestataire, peut donc avoir un impact direct sur l'entreprise. Par la même occasion, une **attaque des outils informatiques d'un prestataire** (**D6**) peut être une porte d'entrée pour une infection du système informatique de EIG France. Un exemple récent est celui de l'attaque de Kayesa (juillet 2021), une société américaine qui fournit des services informatiques à des entreprises : leur logiciel de supervision des flottes de machines de leurs clients a été la cible d'une attaque ; le logiciel a ainsi été transformé en « distributeur de logiciels malveillants » (malwares).

Par ailleurs, dans le cadre de sa communication, EIG France est très active sur les réseaux sociaux. L'**inaccessibilité du compte de l'entreprise sur un réseau social** (**D7**) qui aurait été attaqué, pourrait ralentir son développement commercial.

Enfin, de manière plus large, une **coupure du réseau électrique ou de télécommunication** (**D8**), par acte de malveillance, peut d'évidence mettre à l'arrêt l'activité d'un des sites de EIG France.

6.4.5. Exécution, livraison et gestion des processus

Nous identifions, dans cette catégorie, les risques relatifs aux processus ou relations avec les contreparties commerciales et des fournisseurs.

EIG France, comme tout autre assureur de la place, est tenue de publier des états règlementaires de manière régulière. En cas d'atteinte à son système informatique, EIG France peut être confrontée au risque de **non-publication d'états réglementaires** (**E1**).

Par ailleurs, tout comme pour le retard de règlements de sinistres, EIG France peut, en cas de perturbation d'activité, être sujette à **retard de paiements de prestataires** (**E2**), **retard de paiements de ses charges sociales et fiscales** (**E3**) ou **retard de paiements des salaires des employés** (**E4**).

[36] Une attaque en déni de service ou en déni de service distribué (DDoS pour « *Distributed Denial of Service* » en anglais) vise à rendre inaccessible un serveur par l'envoi de multiples requêtes jusqu'à le saturer ou par l'exploitation d'une faille de sécurité afin de provoquer une panne ou un fonctionnement fortement dégradé du service. (Source : Cybermalveillance.gouv.fr)

6.5. Impact des mesures d'atténuation par risque

		Risque brut			Risque net	
Identifiant du risque	**Description du risque**	**Occurrence**	**Impact**	**Atténuation du risque**	**Occurrence**	**Impact**
FI1	Modification des garanties des contrats	**	*		**	*
FI2	Modification des limites de délégation (souscription)	**	*		**	*
FI3	Divulgation de données financières	**	**	**[M2]** Renforcer la sécurité des données sensibles **[M4]** Verrouiller l'écosystème informatique	**	**
FI4	Accès à des informations à des fins de transactions financières (délit d'initié)	**	*	**[M2]** Renforcer la sécurité des données sensibles	**	*
FI5	Diffusion d'informations stratégiques à l'extérieur	**	***	**[M2]** Renforcer la sécurité des données sensibles **[M4]** Verrouiller l'écosystème informatique	**	***
FI6	Paiement de fausses commissions	**	*	**[M7]** Détecter et prévenir les comportements malveillants	**	*
FI7	Paiement de faux sinistres	**	*	**[M7]** Détecter et prévenir les comportements malveillants	**	*
FI8	Dissimulation de fraude	**	*	**[M7]** Détecter et prévenir les comportements malveillants	**	*
FI9	Changement de bénéficiaires dans les systèmes	*	*	**[M7]** Détecter et prévenir les comportements malveillants	*	*
FI10	Vol de données	***	***	**[M2]** Renforcer la sécurité des données sensibles **[M4]** Verrouiller l'écosystème informatique **[M7]** Détecter et prévenir les comportements malveillants	**	***
FI11	Cryptage des données (ransomware)	*	***	**[M2]** Renforcer la sécurité des données sensibles **[M3]** Améliorer la sauvegarde **[M4]** Verrouiller l'écosystème informatique **[M7]** Détecter et prévenir les comportements malveillants	*	**

		Risque brut			Risque net	
Identifiant du risque	**Description du risque**	**Occurrence**	**Impact**	**Atténuation du risque**	**Occurrence**	**Impact**
FI12	Destruction de données	*	***	**[M2]** Renforcer la sécurité des données sensibles **[M3]** Améliorer la sauvegarde **[M4]** Verrouiller l'écosystème informatique **[M7]** Détecter et prévenir les comportements malveillants	*	**
FI13	Altération de données informatiques (qualité des données)	**	**	**[M2]** Renforcer la sécurité des données sensibles **[M3]** Améliorer la sauvegarde **[M4]** Verrouiller l'écosystème informatique **[M7]** Détecter et prévenir les comportements malveillants	**	**
FI14	Modification des outils (tarification, détection de fraude, etc.)	*	**	**[M6]** Réduire les comportements de contournement des règles sécuritaires **[M7]** Détecter et prévenir les comportements malveillants	*	**
FE1	Cyber espionnage économique	*	*	**[M1]** Poursuivre la sensibilisation des collaborateurs au risque Cyber **[M2]** Renforcer la sécurité des données sensibles **[M5]** Renforcer la protection du SI contre les intrusions	*	*
FE2	Cyberattaque sur nos clients (faux site internet)	**	**		**	**
FE3	Usurpation de comptes sur les réseaux sociaux	**	**	**[M1]** Poursuivre la sensibilisation des collaborateurs au risque Cyber	*	**
FE4	Vol de données	***	***	**[M1]** Poursuivre la sensibilisation des collaborateurs au risque Cyber **[M2]** Renforcer la sécurité des données sensibles **[M4]** Verrouiller l'écosystème informatique **[M5]** Renforcer la protection du SI contre les intrusions **[M6]** Réduire les comportements de contournement des règles sécuritaires **[M9]** Souscrire une assurance cyber risque	**	***

		Risque brut			Risque net	
Identifiant du risque	**Description du risque**	**Occurrence**	**Impact**	**Atténuation du risque**	**Occurrence**	**Impact**
FE5	Cryptage des données (ransomware)	***	***	**[M1]** Poursuivre la sensibilisation des collaborateurs au risque Cyber **[M2]** Renforcer la sécurité des données sensibles **[M3]** Améliorer la sauvegarde **[M4]** Verrouiller l'écosystème informatique **[M5]** Renforcer la protection du SI contre les intrusions **[M6]** Réduire les comportements de contournement des règles sécuritaires **[M9]** Souscrire une assurance cyber risque	**	**
FE6	Destruction de données	***	***	**[M1]** Poursuivre la sensibilisation des collaborateurs au risque Cyber **[M2]** Renforcer la sécurité des données sensibles **[M3]** Améliorer la sauvegarde **[M4]** Verrouiller l'écosystème informatique **[M5]** Renforcer la protection du SI contre les intrusions **[M6]** Réduire les comportements de contournement des règles sécuritaires **[M9]** Souscrire une assurance cyber risque	**	**
FE7	Altération de données informatiques (qualité des données)	***	**	**[M1]** Poursuivre la sensibilisation des collaborateurs au risque Cyber **[M2]** Renforcer la sécurité des données sensibles **[M3]** Améliorer la sauvegarde **[M4]** Verrouiller l'écosystème informatique **[M5]** Renforcer la protection du SI contre les intrusions **[M6]** Réduire les comportements de contournement des règles sécuritaires **[M9]** Souscrire une assurance cyber risque	**	**
C1	Diffusion de données clients sensibles à l'extérieur	***	****	**[M1]** Poursuivre la sensibilisation des collaborateurs au risque Cyber **[M2]** Renforcer la sécurité des données sensibles	**	***

		Risque brut			Risque net	
Identifiant du risque	**Description du risque**	**Occurrence**	**Impact**	**Atténuation du risque**	**Occurrence**	**Impact**
				[M4] Verrouiller l'écosystème informatique **[M5]** Renforcer la protection du SI contre les intrusions **[M6]** Réduire les comportements de contournement des règles sécuritaires **[M8]** Réduire les risques relatifs à la sous-traitance **[M9]** Souscrire une assurance cyber risque		
C2	Retard de paiements des sinistres	***	**		***	**
C3	Gestion d'une demande de rançon (ransomware)	***	***	**[M1]** Poursuivre la sensibilisation des collaborateurs au risque Cyber **[M2]** Renforcer la sécurité des données sensibles **[M4]** Verrouiller l'écosystème informatique **[M5]** Renforcer la protection du SI contre les intrusions **[M6]** Réduire les comportements de contournement des règles sécuritaires **[M9]** Souscrire une assurance cyber risque	**	**
C4	Non-conformité à la réglementation	**	***	**[M2]** Renforcer la sécurité des données sensibles **[M9]** Souscrire une assurance cyber risque	**	**
C5	Absence de réponse aux clients	***	**	**[M5]** Renforcer la protection du SI contre les intrusions	***	**
D1	Interruption des systèmes informatiques (serveurs)	***	***	**[M1]** Poursuivre la sensibilisation des collaborateurs au risque Cyber **[M5]** Renforcer la protection du SI contre les intrusions **[M6]** Réduire les comportements de contournement des règles sécuritaires **[M9]** Souscrire une assurance cyber risque	**	**
D2	Indisponibilité des outils (logiciels)	***	**	**[M1]** Poursuivre la sensibilisation des collaborateurs au risque Cyber **[M5]** Renforcer la protection du SI contre les intrusions	**	**

		Risque brut			Risque net	
Identifiant du risque	**Description du risque**	**Occurrence**	**Impact**	**Atténuation du risque**	**Occurrence**	**Impact**
				[M6] Réduire les comportements de contournement des règles sécuritaires		
D3	Inaccessibilité du site internet de l'entreprise (DDoS)	***	**		***	**
D4	Piratage du site internet de l'entreprise	**	**		**	**
D5	Inaccessibilité des logiciels d'un prestataire (SaaS)	**	**		**	**
D6	Infection d'un outil informatique d'un prestataire	**	**		**	**
D7	Inaccessibilité du compte de l'entreprise sur un réseau social	***	**	**[M1]** Poursuivre la sensibilisation des collaborateurs au risque Cyber	**	**
D8	Blackout (attaque du réseau électrique et de télécommunication)	*	***		*	***
E1	Non-publication d'état règlementaire	*	**		*	**
E2	Retard de paiements à un prestataire	**	**		**	**
E3	Retard de paiements des charges sociales et fiscales	**	**		**	**
E4	Retard de paiements des salaires des employés	*	***		*	***