Mémoire présenté le :

pour l'obtention du Diplôme Universitaire d'actuariat de l'ISFA et l'admission à l'Institut des Actuaires

Par : **Gaëtan Beaud de Brive**

Titre :**Modélisation du risque cyber pour un portefeuille d'assurance français**

Confidentialité : ☐ NON ☒ OUI (Durée : ☐ 1 an ☒ 2 ans)
Les signataires s'engagent à respecter la confidentialité indiquée ci-dessus

Membres présents du jury de l'Institut des Actuaires — *Signature*

. . . . . .

. . . . . .

. . . . . .

Membres présents du jury de l'ISFA

. . . . . .

. . . . . .

. . . . . .

Entreprise :
Nom : **Aon France**

Signature :

Directeur de mémoire en entreprise :
Nom : **Fabien Ramaharobandro**

Signature :

Invité :
Nom :

Signature :

Autorisation de publication et de mise en ligne sur un site de diffusion de documents actuariels *(après expiration de l'éventuel délai de confidentialité)*

Signature du responsable entreprise

Signature du candidat

Mots clés : risque cyber, assurabilité, réassurance, exposition silencieuse, risque de cumul, interconnexion, modèle "fréquence × coût", méthode de Monte Carlo, scénario Black-out, vol de données.

Résumé

Le risque cyber désigne toute menace de perte financière, de perturbation ou d'atteinte à la réputation de particuliers ou de professionnels, due à une défaillance de ses systèmes informatiques. Que ce soit une attaque à proprement parler ou un incident technique, l'omniprésence des objets connectés (ordinateurs, *smartphones*, tablettes, ...) et l'ultra-dématérialisation de l'information ont rendu primordiale la protection des réseaux.

Il s'agit d'une menace complexe qui ne cesse d'évoluer, dont les formes d'expression et les types de pertes sont très variés. Les exemples historiques sont nombreux et montrent bien l'impact que peut avoir une intrusion informatique sur un individu, une entreprise, ou même un gouvernement. Ce risque progresse en parallèle avec les lois et règles de protection mais sa connaissance mathématique reste un challenge majeur pour les acteurs du marché assurantiel.

Ce mémoire a pour ambition de fournir des éléments sur la compréhension actuarielle du risque informatique et son marché, puis de présenter la construction et l'application de plusieurs modèles dans un référentiel français. Nous proposerons dans un premier temps un état des lieux du cyber (le marché assurantiel, la définition du risque et ses caractéristiques, la réglementation et les moyens de défense) qui sera enrichi par une étude des critères d'assurabilité de ce risque (conditions mathématiques mais également sociales, politiques ou encore légales). La conclusion d'une assurabilité théorique limitée mais autorisée par la loi et par le marché explique en partie la présence de produit d'assurance peu adaptée. Nous identifions ainsi les principales particularités qui en font une menace difficile à appréhender : le manque de données, le caractère évolutif, l'exposition souvent silencieuse des entreprises et le risque de cumul.

D'autre part, la proposition d'offres d'assurance sur le marché invite les assureurs à tarifer et modéliser leur exposition. Dans ce mémoire, nous proposerons plusieurs approches de modélisation, en prenant en compte les spécificités du risque cyber. La création d'un scénario déterministe d'accumulation sur un Black-out en Île-de-France viendra combler un manque de modélisation sur le marché français, et nous permettra de déterminer le risque porté par un portefeuille de garanties. En effet, ce type d'approche est conseillée lorsqu'il s'agit d'aborder une nouvelle branche de risque, et particulièrement utile pour mesurer le risque de cumul dû aux grandes interconnexions des réseaux : nous obtiendrons une sinistralité assurantielle d'environ 40m EUR pour la perte d'exploitation sur notre portefeuille, particulièrement impacté sur les secteurs de la finance, l'industrie

et des services aux entreprises.

Nous construirons ensuite un modèle "fréquence × coût" plus classique. Nous modéliserons le risque de "*data breach*" (c'est à dire la violation de données) à l'aide d'une base d'incidents cyber recensés, en intégrant les particularités du marché français et l'interconnexion des réseaux informatiques. Devant la difficulté d'étudier des données françaises, nos lois seront paramétrées sur des données américaines, avant d'être adaptées au marché français. Ainsi, la fréquence annuelle de *data breach* est estimée par une loi Binomiale Négative à partir d'une base de donnée de RBS [1]. De plus, la distribution du coût moyen est calibrée en deux temps : d'une part le nombre d'enregistrements de la base de données, estimé par une loi Logistique et d'autre part le coût moyen unitaire d'une information confidentielle, généré par une loi Normale, centrée sur 146 EUR. L'adaptation aux spécificités du marché français avec des données du *Ponemon Institute* indiquera une inflation du facteur de fréquence de +15% et de la taille moyenne de la base de données de -20%.

Enfin, nous conclurons notre rapport en mesurant, par la méthode de Monte Carlo, l'exposition cyber d'un portefeuille fictif d'assurances, avec les différentes approches créées, dans le but d'estimer une tarification des couvertures d'assurances. Le modèle pour le risque de violation de données nous donne une sinistralité d'environ 27,3m EUR. Dans notre dernier modèle, nous incluons une prise en compte de l'interconnexion, rendue nécessaire par les quasi-monopoles des fournisseurs de logiciel, de serveur et par le partage des réseaux informatiques : nous obtenons une perte globale d'environ 31,9m EUR, soit un écart de +17%.

Les résultats présentés nous permettent de conclure sur la performance du modèle par scénario pour estimer le risque de cumul et l'exposition cyber notamment pour la perte d'exploitation. D'autre part, la mesure du risque de *data breach* par le modèle "fréquence × coût" construit pour le marché français est satisfaisante. Cependant, ces deux approches exigent la prise d'hypothèses importantes et échouent à prendre en compte toutes les spécificités du risque numérique. Adaptés pour introduire le calcul d'exposition de portefeuille de garanties, ces modèles doivent être remplacés par de nouvelles approches incluant des experts du réseau informatique et du risque cyber.

1. *Risk Based Security* est une entreprise qui fournit des informations et analyses détaillées sur les violations de données, voir partie 6.2, page 65.

Key words : cyber risk, insurability, reinsurance, silent exposure, interconnections, risk of cumulation, frequency/severity model, Monte Carlo method, Black-out scenario, data breach.

Abstract

Cyber risk refers to any threat of financial loss, disruption or reputational damage of individuals or professionals, due to a failure of its computer system. Whether it is an attack or a technical incident, the ubiquity of connected devices (computers, smartphones, tablets, ...) and the ultra-dematerialization of information have made the protection of networks essential.

It is a complex and constantly evolving threat, with a wide variety of forms of expression and types of loss. The historical examples are numerous and clearly show the impact that a computer intrusion can have on an individual, a company, or even a government. This risk increases side by side with the laws and protection rules but its mathematical knowledge remains a major challenge for the actors of the insurance market.

The aim of this paper is to provide information on the actuarial understanding of IT risk and its market, before building and applying several models from a french perspective. We will first work on an inventory of cyber (the insurance market, the definition of this risk and its characteristics, regulations and means of defense) which will be completed by a study of the insurability criteria of this risk (mathematical conditions but also social, political or even legal). The conclusion of a theoretical insurability limited but authorized by law and by the market partly explains the presence of unsuitable insurance product. We thus identify the main features that make it a threat difficult to grasp : the lack of data, its evolving nature, silent exposure, and the risk of accumulation.

On the other hand, the proposition of insurance offers on the market invites insurers to price and model their exposure. In this thesis, we will propose several modeling approaches with varying degrees of sophistication, taking into account the specificities of the cyber threat. The creation of a deterministic scenario of accumulation on a blackout in Île-de-France (France) will fill a lack of modeling on the French market, and will allow us to determine the risk carried by a portfolio of guarantees. Indeed, this type of model is recommended when it comes to approaching a risk on a new line of business, and particularly useful for measuring the risk of accumulation due to the large interconnections of the networks : we will obtain an insurance loss of around 40m EUR for the operating loss on our portfolio, particularly impacted on the financial, industrial and business services sectors.

We will then build a more classic "frequency $\times$ severity" model. We will model the risk of data breach using a database of identified cyber incidents, integrating the particularities of the French

market and the interconnection of computer networks. Faced with the difficulty of studying French data, our laws will be configured on American data, before being adapted to the French market. Thus, the annual frequency of data breach is estimated by a Negative Binomial distribution from an RBS [2] database. In addition, the distribution of the average cost is calibrated in two stages : on the one hand the number of records in the database, estimated by a Logistics distribution and on the other hand the average unit cost of a confidential information, generated by a Normal distribution, centered on EUR 146. The adaptation of our work to the French market with data from the Ponemon Institute will indicate a +15% inflation of the frequency factor and a -20% deflation of the average size of the violated database.

Finally, we will conclude our report by measuring, using the Monte Carlo method, the cyber exposure of an insurance portfolio, with the different approaches created, with the aim of pricing the insurance cover. The data breach model gives us a result of around EUR 27.3m. In our last model, we include a consideration of the deep network interconnection, made necessary by the monopoly of the suppliers of softwares, of servers and by the sharing of computer networks : we obtain a global loss of approximately EUR 31.9m, so an increase around +17 %.

The results presented allow us to conclude on the performance of the "Blackout scenario" model to estimate the risk of accumulation and cyber exposure especially for the operating loss. On the other hand, the measure of the risk of data breach by the "frequency $\times$ severity" model constructed for the French market is satisfactory. However, these two approaches require important assumptions and fail to take into account every specificities of the IT risk. Adapted to introduce the calculation of portfolio exposure, these models need to be improved by new approaches that include computer network scans and cyber risk experts.

2. *Risk Based Security* is a company who provides detailed information and analysis on data breaches, see part 6.2, page 65.

Remerciements

Je souhaite remercier Fabien Ramaharobandro, Nadia Hager et Alima Badji pour leur accueil et leur encadrement au sein d'*Aon Reinsurance Solutions* de Aon France. J'aimerais également remercier l'équipe Analytics pour leur soutien, particulièrement à Imane Hamny, Quentin Huin Morales et Tristan Trouillard.

Je tiens à remercier Aurélien Couloumy pour son encadrement en tant que tuteur académique, ainsi que les professeurs de l'ISFA pour leur accompagnement pendant ces trois dernières années. Je profite de ce paragraphe pour adresser mes remerciements aux professeurs qui m'ont accompagné tout au long de ma vie scolaire, et m'ont transmis leur attrait pour les mathématiques et l'actuariat, particulièrement messieurs Frédéric Laroche et Bruno Harington.

Et enfin, je tiens à exprimer mon éternelle reconnaissance à mes amis et ma famille, à mes parents et frères et soeur, pour leur patience et leur bienveillance.

Introduction

Le risque cyber désigne toute incertitude de perte due à une défaillance des systèmes informatiques. Or, ces derniers font désormais partie intégrante de nos quotidiens personnels et professionnels. Les ordinateurs, mais également les *smartphones* sont devenus quasiment indispensables dans nos modes de vie et contiennent des informations sensibles. Que ce soit une attaque à proprement parler ou un incident technique, le risque informatique atteint donc toute entité qui exploite un réseau numérique, tout appareil possédant une puce électronique, quel qu'il soit.

Ainsi, la menace évolue sans arrêt, parallèlement aux progrès techniques. De plus, la difficulté à diagnostiquer une intrusion accroît l'exposition à ce danger : il faut attendre en moyenne sept mois avant qu'une entreprise ne réalise qu'elle a été la cible d'un piratage [3]. La sécurisation de ses réseaux de données est un enjeu devenu majeur pour les entreprises. Les moyens de protection informatique n'étant pas suffisants, le transfert de risque à des professionnels est nécessaire. Par conséquent, les assureurs se retrouvent face au défi d'offrir une réponse adaptée et efficace à ce danger.

Nous travaillerons donc dans un premier temps sur un état des lieux du cyber avec une présentation concise de ce domaine : le marché assurantiel et ses caractéristiques, les différentes catégories et victimes. Nous travaillerons sur l'aspect réglementaire et les moyens de protection. Enfin, les challenges et points d'attention dans la modélisation du risque cyber seront présentés en un second temps et nous inviterons à nous poser la question de l'assurabilité d'un tel risque.

Pour finir, nous présenterons les étapes de construction de plusieurs modèles actuariels d'appréhension de ce risque : les bases de données utilisées, les méthodes choisies et les hypothèses prises. Nous introduirons ainsi une approche "par scénario", puis un modèle "fréquence $\times$ coût", avant de proposer des résultats prenant en compte le risque d'accumulation. L'objectif de ce chapitre est de réussir à modéliser la menace cyber et d'appliquer une tarification adaptée pour un portefeuille d'assurance, mais également de comparer nos résultats et d'identifier les limites dans nos modélisations.

L'ensemble des calculs et résultats présentés dans ce rapport ont été réalisés sous R.

3. Source : "*Les attaques cyber en quelques chiffres*", Data-it.fr 2019.

Table des matières

Première partie

Présentation d'un risque nouveau, enjeux et difficultés de modélisation

1 Introduction au risque cyber

1.1 Introduction et catégories de risques cyber

Un risque pour une entreprise est la possibilité d'occurrence d'un évènement qui pourrait compromettre son activité, entraver sa pérennité. En effet, le risque est un préjudice, un sinistre éventuel que les compagnies d'assurance garantissent moyennant le paiement d'une prime. On peut également citer la littérature assurantielle classique qui propose une définition du risque comme la formule mathématique suivante [12] :

$$\textbf{Risque} = \textbf{Probabilité} \times \textbf{Amplitude}$$

On considère ainsi le risque comme la combinaison de la probabilité d'un évènement de perte et l'amplitude de cette sinistralité. Le risque est la multiplication entre l'aléa (probabilité et intensité) et la gravité (intensité et vulnérabilité). Cette définition souffre de plusieurs défauts mais a la qualité d'être simple.

Mais alors, quels risques peuvent être qualifiés de "cyber" ? Sur ce point les experts ne sont pas forcément unanimes. Nous estimerons dans cette étude qu'il doit y avoir implication du réseau [18] [5] pour venir voler des données, endommager des logiciels ou bien même simplement espionner l'activité de manière non autorisée. Par ailleurs, l'intrusion doit être effectuée dans un but malveillant [4] pour qu'on puisse évoquer une attaque cyber. Certains chercheurs émettent la différence entre un risque cyber et un risque non-cyber sur la forme [27] et d'autre sur la cible [6] [3] : une distinction entre la fin et le moyen. En s'intéressant à la fin, on pourrait définir cette menace comme ce qui "touche à la violation de données, ou à une intrusion sur le réseau, et résulte en la détérioration ou le vol matériel ou immatériel d'actifs" [5]. On comprend déjà dans la définition même du risque cyber que la création d'un produit pour le couvrir va être délicate. L'approche que nous avons choisie dans cette étude se veut générale et en cohérence avec les hypothèses du marché : le terme "cyber" [6], désigne le domaine interactif composé de l'intégralité du réseau numérique utilisé pour emmagasiner, travailler, et transmettre de la donnée. Cela implique donc l'ensemble des systèmes d'informations utilisés de manière personnelle et professionnelle. Enfin, l'interconnexion généra-

4. D'après le site internet du gouvernement Français, source : *info.gouv.fr*, 2019.
5. Inspiré de l'Argus de l'Assurance, 2012.
6. Vient du "*cyberspace*", néologisme anglais des années 1980.

lisée des ordinateurs et plateforme de stockage et d'échange dans le monde explique l'étendue de la menace cyber, et l'évolution permanente des technologies expliquent (en partie) sa complexité d'appréhension.

Les catégories de risque cyber

Pour mieux saisir la signification d'un risque cyber, on peut le présenter sous plusieurs catégories et ainsi voir ce que représente cette menace informatique. Le tableau ci-après répertorie les classes de risque cyber [6].

Catégorie	Description	Éléments
Sous-catégorie 1 : Actions humaines		
1.1 Involontaire	Action non-intentionnelle effectuée sans volonté de nuire.	Erreur par omission.
1.2 Délibérée	Action intention elle effectuée avec la volonté de nuire.	Sabotage, fraude, vol, vandalisme.
1.3 Inaction	Réponse inadaptée face à une situation dangereuse.	Manque de compétence appropriée, de connaissance personnelle, d'anticipation.
Sous-catégorie 2 : Défaillance du système / de la technologie		
2.1 Matériel	Risques dûs aux défaillances des équipements physiques.	Problème de capacité, d'obsolescence, de maintenance.
2.2 Logiciel	Risques découlant des logiciels de tous types (programmes, applications, systèmes d'exploitation).	Compatibilité, gestion de configuration, paramètres et réglages de sécurité et tests.
2.3 Système	Défaillance de certains systèmes.	Performance altérée, cahier des charges inadapté.
Sous-catégorie 3 : Erreur dans le processus interne		
3.1 Conception & Exécution	Risque opérationnel : incapacité du processus à traiter la demande.	Problème de flux d'informations, notifications, transferts de tâches.
3.2 Contrôle	Contrôle de l'opération non-adapté.	Surveillance des étapes, mesures intermédiaires, etc.
3.3 Pilotage	Défaut dans le pilotage/l'emploi des ressources appropriées.	Continuité du développement, formation des salariés.
Sous-catégorie 4 : Évènements extérieurs		
4.1 Dangers généraux	Évènements naturels ou humains où l'entreprise n'a aucun contrôle	Tous types d'évènements naturels, incendie, inondation, etc.
4.2 Législation	Risque résultant de la légalité.	Conformité réglementaire, procès...
4.3 Problèmes commerciaux	Risque résultant du changement d'environnement commercial de l'entreprise.	Défaut d'un fournisseur, changement d'état du marché, crise économique
4.4 Dépendances du service	Risques dus à la dépendance de l'entreprise	Locaux, services d'urgences, transport.

Table 1 – Les catégories du risque cyber

Notre définition nous invite à nous pencher plus précisément vers les intrusions volontaires extérieures : nous nous concentrerons dans ce mémoire sur les attaques cyber. Son exposition

concerne tous les réseaux informatiques, et de manière générale tout appareil disposant d'une puce électronique, donc tous les utilisateurs d'ordinateur, soit l'intégralité du marché. Dès lors, la menace est omniprésente et nécessite une bonne organisation de protection, une gestion de risque appropriée. L'attaque cyber peut cibler aussi bien des unités centrales que des serveurs (isolés ou en réseaux) ou des équipements périphériques comme les scanners, imprimantes, téléphones, etc. Ainsi, les conséquences d'une attaque cyber peuvent être désastreuses. Certains assauts ont été si particuliers par leur ampleur, leur originalité, ou leur complexité qu'ils sont restés dans les annales. L'historique de sinistralité cyber nous apprend également qu'il existe une grande variation dans les attaques, que ce soit dans les cibles, les motivations ou encore les méthodes utilisées. La connaissance de ces particularités est essentielle pour appréhender le risque auquel les entreprises sont exposées.

1.2 Les attaques cyber : motivations, pertes et victimes

Motivations des attaques

Comprendre la volonté et le but recherché par les pirates peut nous aider à appréhender notre risque, et à s'en protéger. Dans le cas de la criminalité informatique, nous recensons de nombreuses raisons qui peuvent inciter à passer à l'action : nous allons les présenter dans cette partie.

La plus répandue est sûrement la **motivation pécuniaire**. En effet, réussir une attaque cyber peut rapporter beaucoup d'argent. Que ce soit le commerce d'informations confidentielles sur le *Dark Net*, ou la vente directe du fruit du piratage à la concurrence, les données volées peuvent être rentables. Une atteinte cyber visant une entreprise peut entraîner la récupération de données bancaires des utilisateurs du site internet, et ainsi une fraude aux cartes de crédit par exemple. L'**espionnage industriel** est également une offensive informatique des plus répandues.

La volonté d'attaquer une entreprise peut également être dictée par la cible en elle-même : comme nous le comprenons (et le verrons en détail ultérieurement), l'entité victime de criminalité cyber peut voir son image fortement détériorée, sa crédibilité endommagée et par engrenage, sa pérennité. Ainsi, l'agression cyber peut résulter d'une envie de nuire, pour des motivations morales, éthiques ou personnelles : on appelle cela "***hacktivism***" : militantisme informatique, qui résulte en des agressions informatiques envers des entreprises jugées néfastes pour les droits de l'homme, l'environnement, les inégalités sociales, ou tout autre motif de lutte. On retrouve dans ce type de profil des groupes ayant atteint une certaine notoriété comme *Anonymous*, *WikiLeaks* ou encore *Chaos Computer Club*.

La compétition "Pwn2Own" est un concours annuel où des experts en informatique essaient pendant plusieurs jours de pénétrer des systèmes d'exploitation. En effet, certains pirates peuvent

s'en prendre à une entreprise simplement pour **le défi**. De fait, la renommée et la réputation sont importantes dans ce milieu. Certains pirates informatiques ont atteint une célébrité mondiale, comme par exemple le pirate informatique Kevin Mitnick. Les "*script kiddies*" sont, comme leur nom l'indique, les amateurs de *hacking* qui s'amuse à voler des données, avec un certain attrait pour l'interdit. Nourris par le fantasme du cinéma et des livres, certains sont influencés et poussés à l'action par leur imaginaire, dans une quête de divertissement, sans même forcément réaliser qu'ils transgressent les lois.

Ainsi nous comprenons que les motivations sont nombreuses, ce qui illustre encore une fois l'ampleur de la menace cyber. On pourrait aussi citer l'enjeu **politique** [7] lorsque des *hackers* tentent de déstabiliser un gouvernement en place, ou de s'immiscer dans les processus électoraux en divulguant des informations (possiblement des "fake news") par exemple. Les raisons principales sont résumées dans le schéma ci-dessous.

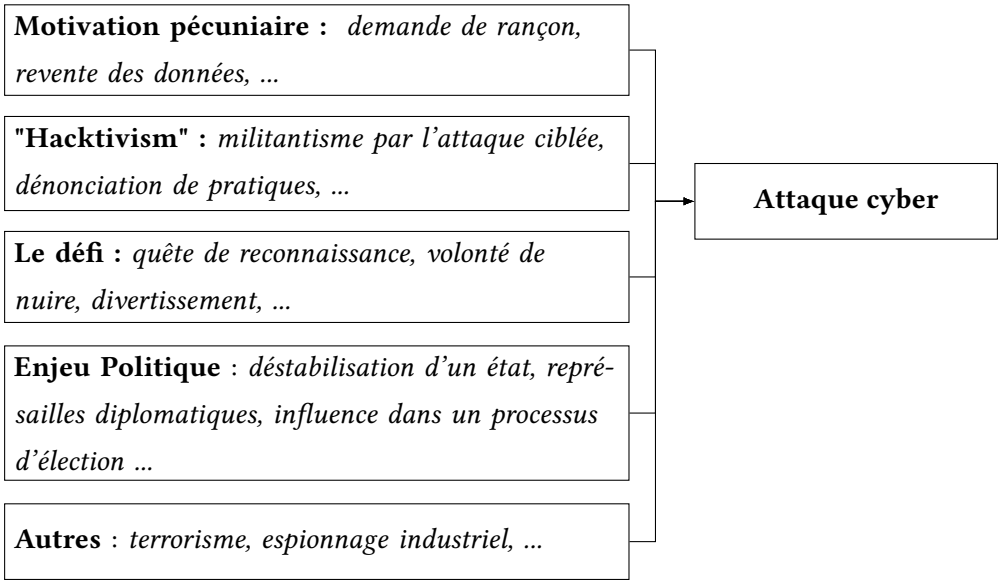


FIGURE 1 – Motivations des attaques cyber

Ces différentes motivations se traduisent de manières variées dans les faits. En effet, la raison qui pousse à passer à l'action va de pair avec les dégâts que l'on veut infliger (ou non) à la cible. Nous pouvons classer les atteintes cyber en fonction de la volonté recherchée par le pirate en quatre différentes catégories :

- L'**idéologie**, la morale (où nous retrouvons les "*hacktivists*") ;
- Les motivations **financières** (rançon, revente des données, ...) ;
- L'**espionnage** (ou "*spying*") ;
- La **destruction** (ou du moins l'interruption d'activité, pour les raisons politiques par exemple).

7. En 2009, les membres du groupe Anonymous créent le site web *Anonymous Iran* et publient un manifeste vidéo à destination du gouvernement Iranien. Action menée aux cotés de *The Pirate Bay*. Source : iran.whyweprotest.net, 2009.

Nous nous servirons ultérieurement de cette classification notamment dans la modélisation par scénario [8].

Un peu d'historique

En plus d'avoir été destructrices, les plus célèbres attaques ont posé les fondations pour les suivantes. En voici quelques exemples [9] :

- **"Stuxnet"** : Exemple d'attaque à enjeu politique, il s'agit d'un virus développé par les autorités israëliennes et américaines afin d'enrayer les recherches iraniennes pour l'arme nucléaire en 2010 ;
- **Target** : Exemple d'attaque de "*data breach*" [10]. La chaîne de grande surface américaine Target est la cible en 2013 d'un piratage de grande envergure et se font dérober plus de 100 millions d'informations confidentielles sur ses clients (adresses mail, numéros de téléphone, coordonnées bancaires, etc.) ;
- **E. Snowden** : Exemple d'*hacktivist* qui a utilisé ses connaissances en informatique pour dévoiler des secrets gouvernementaux des États-Unis, notamment sur des programmes de surveillance de masse en 2013.

A travers ces exemples, nous pouvons illustrer plusieurs points de cette étude : que ce soit l'ampleur du risque, les motivations variées des pirates, l'éventail des pertes subies, la différence dans les types d'attaques et de victimes et enfin l'importance de se protéger face à cette menace. Le risque cyber est émergent, et se décline de plusieurs façons, aussi bien dans les différentes armes employées que dans les cibles atteintes. Le sujet de la partie suivante est donc d'analyser cette menace, ses caractéristiques, sources et conséquences.

L'éventail de victimes

Les victimes d'une attaque cyber peuvent être variées et nombreuses. Nous pouvons notamment souligner le fait qu'il existe des victimes directes et indirectes : par exemple, dans le cas d'un *data breach* (ou "perte/vol de données"), la victime directe est l'entreprise ciblée, et la victime indirecte le particulier dont les informations confidentielles ont été dérobées (et pourront être utilisées, à son insu). Cet éventail de victimes potentielles est à prendre en compte dans nos modélisations et dans la calibration d'une couverture assurantielle.

Types d'attaques et pertes infligées

De manière générale, pour réussir à pénétrer un lieu protégé, il existe deux façons de procéder : la première méthode est d'adapter l'attaque à la défense, c'est-à-dire utiliser des outils adaptés pour

8. Voir partie "Scénario Black-out Île de France".
9. Plus de détail en annexe A : "quelques exemples marquants".
10. Vol/perte de données par intrusion informatique.

la tâche. Exploiter une faille qui n'a pas encore été résolue par les développeurs du logiciel s'appelle une attaque sur la vulnérabilité *0-day*. La seconde procédure est de trouver un allié qui peut nous faire rentrer depuis l'intérieur. Ce correspondant n'est pas forcément conscient de son aide : la personne peut être simplement mal formée ou naïve, et va par ses actions, faciliter la pénétration du système. C'est le cas le plus fréquent lors d'un sinistre cyber : 90% des pertes cyber sont dues à des erreurs humaines [15]. Ainsi, sensibiliser les employés et le grand public à cette menace pourrait permettre d'éviter beaucoup de dégâts. Dans cette sous-partie nous allons nous pencher sur les différents types d'attaques et puis sur les pertes qu'elles peuvent engendrer.

Les formes d'attaques cyber

La menace cyber se décompose en un éventail de différents risques et outils. Connaître leur existence et comprendre leur moyen de fonctionnement permet une meilleure gestion et surtout une protection plus efficace, que ce soit dans le cadre professionnel ou dans la vie privée. Nous allons présenter ici quelques formes très classiques d'intrusion cyber [11] :

- **Malwares** : Un programme malveillant ("*malware*" ou "maliciel") désigne tout type de logiciel essayant d'infecter un objet connecté (ordinateur, téléphone mobile par exemple). Les attaquants se servent de maliciels pour extraire des informations ou des codes d'accès, détourner de l'argent ou bloquer l'utilisation de l'appareil. Des logiciels existent pour s'en protéger ;
- **Spying** : Un logiciel espion est un type de maliciel dont se servent les pirates pour espionner afin d'obtenir des données personnelles (bancaires par exemple), ou des informations de connexion (sites visités, durée, etc.) ;
- **Hameçonnage** (*phishing*) : L'hameçonnage (appelé également "*phishing*") consiste à inviter la cible à révéler des informations sensibles par un *e-mail* ou un site internet factice, en se faisant passer pour quelqu'un de légitime ;
- **Ransomware** [12] : les logiciels de rançon fonctionnent comme une prise d'otage : le logiciel force l'entrée et bloque l'accès à l'information (base de données, outils, ...). Il demande ensuite le règlement monétaire (souvent en cryptomonnaie du type *Bitcoin*) pour s'extraire.

Voilà une courte liste d'attaques récurrentes que l'on peut observer parmi les sinistres cyber les plus fréquents. On aurait tendance à penser que les attaques cyber se concentrent uniquement sur le vol de données, le piratage de logiciels ou le détournement de fond, mais la réalité est toute autre : en effet, les intrusions informatiques peuvent être effectuées dans le but d'une atteinte physique.

Une illustration concrète, récente et française est l'intrusion cyber de 2015 qui a atteint l'hydrolienne *Sabella* sur les côtes bretonnes : le virus a endommagé la liaison avec le centre de contrôle

11. Nous présentons en annexe une liste plus complète de ces menaces informatiques. Voir annexe D : "éventail des méthodes de piratage informatique".

12. Nous choisissons volontairement de laisser le mot anglais, que l'on retrouve bien plus fréquemment que sa traduction "rançonlogiciel", même dans la littérature francophone.

rendant impossible son exploitation. Une rançon a été réclamée pour lever le cryptolocker [13]. Il existe d'autres exemples, et diverses méthodes qui sont développés en annexes du présent rapport- Voir Annexe E : "éventail des méthodes de piratage informatique (dommage au bien)".

Types de pertes infligées

Ainsi nous voyons que de nombreux types de manipulations existent. Ces menaces vont de pair avec la volonté de perte à infliger : que ce soit pour en tirer profit ou pour déstabiliser sa cible, il existe un large panel de dégâts possibles.En effet, les dommages résultant d'une attaque cyber peuvent être matériels (robots d'usine à réparer, ordinateurs endommagés), immatériels (base de données, espionnage industriel), quantifiables (perte d'exploitation, détournement de fond), non-quantifiables (atteinte à l'image, à la réputation, perte de clientèle) : ils peuvent donc impacter différentes polices d'assurances (dommage, responsabilité civile, etc.).

1.3 Protection, réglementation et assurances

Cyber Hygiene : Comment se protéger contre le risque cyber ?

La *cyber hygiene* fait référence aux pratiques et étapes suivies par les utilisateurs (entreprises et particuliers) d'ordinateurs (et outils connectés) pour maintenir la santé du système et en améliorer la sécurité [14]. Dans le cadre des assurances cyber, on peut imaginer une mesure de cette grandeur hygiénique afin d'appliquer des critères sur les couvertures et leur prix.

Certains algorithmes commencent à voir le jour dans ce but : par exemple, *Homeland Security* [15] utilise les données du marché pour compiler des scores informatiques à l'aide d'un algorithme appelé "AWARE" [16]. L'algorithme mesure l'existence de vulnérabilités connues dans les systèmes d'une agence (ceux qui n'ont pas encore été corrigés) et les paramètres de configuration de base permettant de donner à une agence une évaluation globale de son hygiène cyber [17]. De même, l'entreprise indépendante *BitSight* propose des notes de sécurité informatique dans un but assurantiel, tout comme les notations pour les emprunts bancaires par exemple.

Ainsi, le *cyber hygiene* est l'ensemble des procédés permettant à une entreprise ou un particulier de protéger sa machine connectée. Nous pouvons les séparer en deux grandes catégories : les actions directes (des mesures évidentes jusqu'aux moyens techniques complexes) et les actions indirectes (comme le transfert assurantiel de risque).

13. Source : "L'hydrolienne Sabella bloquée par un virus chiffreur" Science et Avenir, 2016.
14. Source : Digital Guardian, 2018.
15. Département de la sécurité intérieure des États-Unis.
16. Acronyme anglophone pour "*Agency-Wide Adaptive Risk Enumeration*".
17. Source : *"Agencies Will Soon Have a Cyber Hygiene Score"*, Aaron Boyd, 2018.

Actions directes

Par opposition à la gestion du risque "indirecte" comme le transfert à l'assurance, ou la prévention, on appelle actions directes les méthodes de *cyber hygiene* que l'utilisateur met en place lui même : elles peuvent être relativement basiques ou bien techniques.

Les actions directes simples dans le cas du cyber sont la modification régulière des mots de passe et des numéros d'identification de connexion, des choix de clés de sécurité différentes et complexes (le nombre de caractère et les symboles employés notamment). Ces réflexes de base permettent de diminuer grandement l'exposition à un piratage informatique. De même, il convient de ne pas se connecter sur les réseaux publics, de faire les mises à jour régulièrement et de sauvegarder ses travaux sur ports externes (CD ou USB), en faisant des copies. On comprend donc également la nécessité de la prévention et de la sensibilisation [18].

Il existe également des méthodes plus techniques comme les antivirus, le *firewall*, le *honeypot*, ou encore le chiffrement des données par exemple [19] qui limitent les intrusions externes indésirables. Nous avons ainsi présenté (brièvement) quelques méthodes, certaines de base et d'autres plus élaborées de protection contre une perturbation cyber. Il convient de tout de même relever que ces boucliers ne sont pas suffisants, même s'ils permettent de limiter l'exposition, ce qui est toujours souhaitable. Les entreprises et individus restent de manière générale très vulnérables dans ce domaine. Les assurances ont donc un rôle majeur à jouer dans le transfert de ce risque en proposant une couverture adaptée.

Actions indirectes : l'importance d'une couverture d'assurance et de réassurance

Face à la nature complexe et évolutive d'un tel risque, le pouvoir de réponse des assureurs reste limité. Et pourtant, l'assurance porte un enjeu fondamental dans la gestion de cette menace. En effet, la souscription à une protection présente plusieurs atouts : en plus de contraindre les entreprises clientes à effectuer un état des lieux et une cartographie des risques cyber auxquels elles sont exposées, elle a pour objectif de protéger l'activité de ces dernières en couvrant les pertes que la prévention n'a pas réussi à esquiver. Or, les acteurs économiques en France sous-estiment leur exposition à la menace digitale et donc ne se tournent pas (suffisamment) vers le transfert du risque aux assurances. Il y a plusieurs raisons qui expliquent une erreur d'une telle ampleur : la méconnaissance de la nature du danger et des dommages qu'il pourrait causer, l'ignorance de l'existence des contrats qui leurs sont proposés. Près de 50% des dirigeants d'entreprises européennes affirmaient en 2016 ne pas connaître l'existence de police de protection pour le risque cyber, et 73% n'en auraient qu'une connaissance limitée [20]. Ainsi, ce renseignement limité constitue un frein sévère à

18. On estime à 90% les sinistres déclarés résultant d'une erreur humaine [15].
19. Sujets développés en annexe F : "*Cyber hygiene*, solutions de protection des machines connectées".
20. Source : Lloyd's of London, *Facing the Cyber threat*, 2016.

la souscription. De plus, le risque de cumul entraîné par l'importante interconnexion des expositions des entreprises au risque cyber rend nécessaire l'appel à la réassurance pour les compagnies d'assurance.

L'environnement réglementaire du risque cyber

Classé en tête du baromètre des risques émergents pour le secteur de l'assurance et de la réassurance cette année par la FFA [21], la menace cyber est prise au sérieux par les organes d'autorités. C'est dans ce contexte que la France et l'Europe se sont dotés d'un arsenal de réglementations nationales et internationales pour d'une part protéger les individus et leurs données, et d'autre part accompagner et encadrer les entreprises dans leur gestion du risque informatique.

Introduisons tout d'abord en précisant que la législation mondiale est d'une part assez inégale en fonction des zones géographiques, et en plein développement. La carte [22] ci-dessous représente l'avancée des législations concernant la protection des systèmes d'information face au risque informatique dans le monde.

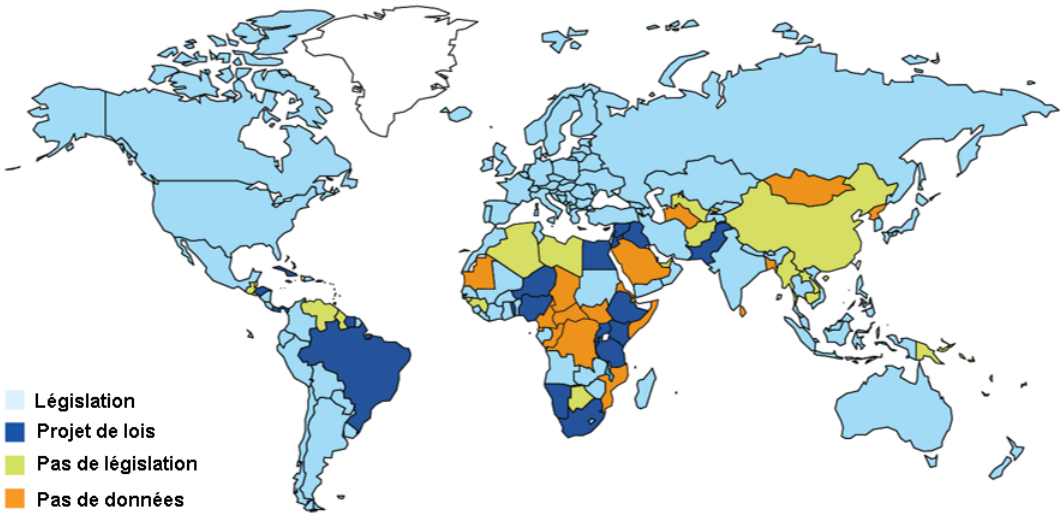


FIGURE 2 – Législation mondiale concernant la législation cyber, 2016

Les règles et normes en vigueur

Ces règles s'appliquent aussi bien dans le cadre de l'utilisation des données, que de leur protection ou des obligations de notification en cas d'intrusion. Cette législation a pour but d'harmoniser les règles en France et en Europe, mais également et surtout, de protéger les individus et les entreprises.

21. fédération française de l'assurance, 2019.
22. Global CyberLaw, CNUCED, Décembre 2016.

Nous pouvons citer en premier lieu la norme de sécurité de l'information *ISO/CEI 27000* qui régissent la protection des bases de données. Le règlement général sur la protection des données (RGPD) est également un texte majeur dans la réglementation cyber, qui dicte notamment les obligations de notification et les méthodes d'anonymisation des informations confidentielles ou sensibles. Il existe également des directives sur l'utilisation de certains outils connectés, comme la PCI DSS (norme de sécurité de l'industrie des cartes de paiement), ou encore la DSP (directive sur les services de paiement).

Cette présentation des règles concernant la gestion du risque cyber n'est pas exhaustive. Nous pouvons préciser qu'il s'agit aussi bien de cadres législatifs que de guides pour aider les entreprises à adapter leur gestion. Enfin, nous pouvons conclure cette section en précisant qu'il n'existe pas de ligne d'activité (*Line of Business*) concernant directement la protection cyber dans la directive Solvabilité 2 (S2), ce qui semble être un véritable défaut. Pour remédier à cela, les entreprises doivent tout de même quantifier leur exposition pour S2. Pour ce faire, l'exposition est divisée entre le dommage (*First party*) et la responsabilité civile (*Third party).*

Les régulateurs [23]

En ce qui concerne les acteurs principaux de la régulation dans le domaine du risque cyber, nous pouvons tout d'abord citer l'ENISA (Agence européenne chargée de la sécurité des réseaux et de l'information). La CNIL (Commission nationale de l'informatique et des libertés) régule la récupération des données par les entreprises, et est notamment responsable des demandes d'acceptations des *cookies*. L'ANSSI (Agence nationale de la sécurité des systèmes d'information) s'occupe de la défense française des réseaux. L'ACPR (Autorité de contrôle prudentiel et de résolution) joue également un rôle dans le marché assurantiel pour la protection informatique. Notons enfin qu'il existe plusieurs autres entités chargées de la réglementation du risque cyber (Le contrôleur européen de la protection des données (EDPB), Europol, le comité économique et social européen, etc.).

D'autre part, la gouvernance n'est pas forcément extérieure aux entreprises. En effet, même si le contrôle et les sanctions viennent principalement des autorités présentées ci-dessus, au sein même des entreprises des fonctions internes existent pour appliquer le respect du cadre proposé. La mise en oeuvre interne doit être résumé dans une publication regroupant plusieurs documents de référence [24] : la PSSI (Politique de Sécurité du Système d'Information). Il s'agit d'une recommandation commune de l'ANSSI, de l'ACPR et de la CNIL.

23. Sujet développé en annexe G : "Précisions sur la régulation du cyber".

24. Comme par exemple la charte d'utilisation des moyens informatiques, la politique de confidentialité des données, les clauses contractuelles à intégrer dans les accords, etc.

L'assurance cyber

Un marché en pleine expansion

Les assureurs ne communiquent pas vraiment d'informations détaillées sur les primes acquises et les charges payées à propos du cyber. En conséquence, la dimension réelle des transactions de l'assurance cyber est difficile à estimer. Nous allons tout de même présenter dans cette section l'état actuel du marché mondial.

Depuis 2015, le nombre d'attaques cyber recensées a fortement progressé (en France et dans le monde). En parallèle à cette augmentation d'incidents cyber, les dépenses en terme de protection informatique des entreprises ont également gonflé (170 Md USD estimés pour 2020 [25]). En comparaison, la criminalité cyber est estimée par certaines sources à près de 6 Bn (10^{12}) USD de perte annuelle d'ici 2021 [17] (et continuerait de croître), ce qui correspond à un montant supérieur à celui des dégâts causés par les catastrophes naturelles sur une année.

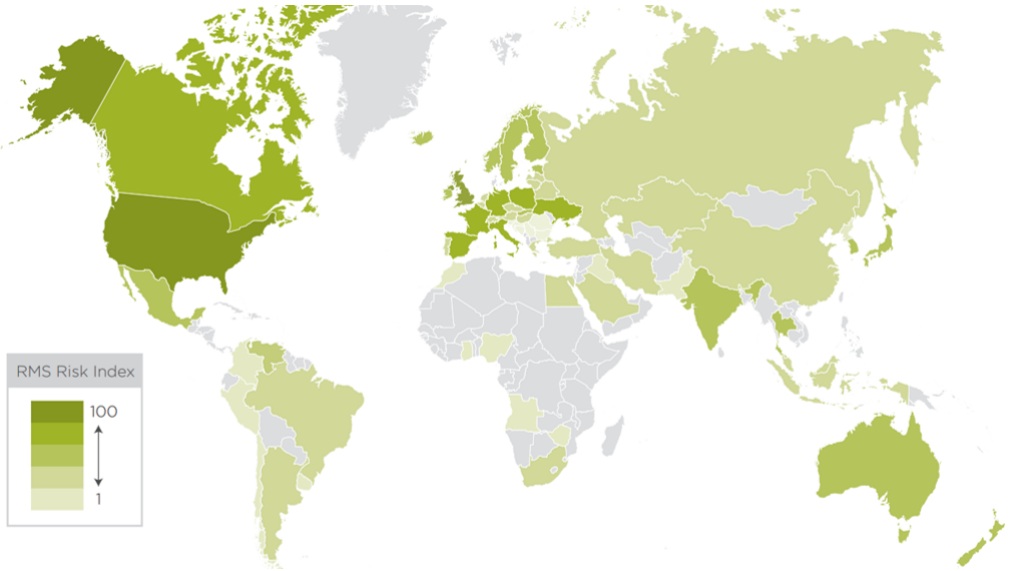


Figure 3 – Le risque cyber à travers le monde

Cette carte [26] représente géographiquement l'indice construit par RMS [27] sur les menaces cyber à travers le monde. Il est tout d'abord important de noter les disparités que l'on constate dans cette activité : les États-Unis se démarquent du reste du monde avec un marché plus développé et en avance sur de nombreux points. Quant à l'Europe (et la France notamment), les efforts pour se mettre à jour sont à prendre en compte, mais le retard reste conséquent.

En effet, le marché américain représente la grande majorité des primes (près de 80%), étant plus

25. Source : Les Echos, "Le marché de l'assurance cyber", 2017.
26. Source : RMS, 2018.
27. RMS : *Risk Management Solution* est l'entreprise leader mondial de la modélisation de catastrophe.

mature et plus avancé en terme de sécurité : les premiers contrats spécifiques au risque cyber étant apparus aux États-Unis dans le début des années 2000. Ils ont connu un essor particulièrement important, poussé par un développement des lois en ce sens. En particulier, les entreprises doivent prévenir les particuliers lors d'un *data breach* impliquant leurs données personnelles (première loi étatique d'obligation de notification signée en 2002 en Californie).

Soulignons d'autre part que l'Europe possède à l'heure actuelle seulement 10% de ce marché en terme de prime. Or, malgré le retard considérable des acteurs français, et européens de manière générale, les compagnies d'assurance et de réassurance de la place poursuivent leur développement vers une meilleure compréhension et gestion de l'exposition au cyber. En effet, l'exigence législative qui va de pair avec la croissance de ce risque constitue une réelle opportunité pour les assureurs. Nous constatons notamment que les principaux assureurs en France proposent désormais des offres cyber ou sont en cours de création de produits [28].

Les contrats et solutions d'assurance

Nous avons donc vu que le marché des assurances cyber était d'une part considérable en terme de transfert de primes et de charges, mais également en plein essor [29]. Nous allons à présent nous pencher sur les types de contrats du marché et sur les couvertures que l'on devrait y trouver[7], c'est à dire quelles indemnisations doivent être proposées par une garantie d'assurance suite à une attaque cyber :

- Tout d'abord, une protection liée à la **cause du sinistre** : prenons l'exemple dans le cas d'une intrusion ou d'un *malware* implanté dans une machine connectée, les frais de nettoyage du système pourraient être couverts par le transfert du risque à l'assurance ;
- Liée à la **conséquence du sinistre** : que ce soit matériel ou non, les réparations qui s'imposent sur les éléments endommagés peuvent être prises en charge par l'assureur. De plus, les paiements des cellules de crise ou des centres de notifications (dans le cadre du RGPD par exemple) semblent pouvoir être à la charge de l'organisme d'assurance ;
- Sous forme de **forfait financier** : Une sorte d'enveloppe d'un montant forfaitaire pour l'entreprise victime de la part de la compagnie d'assurance qui détient la police cyber ;
- Prestation d'assistance et de **service** : une aide en nature par des experts pour les diagnostics ou les installations de défenses supplémentaires par exemple. Le déclenchement d'une cellule de crise et la mise à disposition de personnel.

Voyons à présent ce que nous pouvons trouver sur le marché en terme de couverture pour le risque cyber. D'après nos observations, il existe trois cas distincts qui permettent à une entreprise d'être couverte en cas de sinistre d'origine cyber au sein de son activité [30].

28. Source : Aon, "Les évolutions du marché cyber depuis 18 mois", 2019.
29. Voir annexe I : "Marché d'assurance cyber en France".
30. En ce qui concerne le marché des particuliers, nous présentons ce sujet en annexe J.

Les contrats avec clauses (*Cyber Endorsements*)

Les contrats avec clauses cyber (ou *Cyber Endorsements*) représentent une petite partie du marché cyber en France. Il s'agit d'une clause dans un contrat traitant d'un autre risque. Clause prenant en compte le fait qu'un sinistre puisse être d'origine cyber et donc serait tout de même couvert par ce contrat.

Les contrats spécifiques *(Stand Alone Cyber)*

Il s'agit d'un contrat classique de couverture contre le risque cyber. Cela est très large mais l'avantage d'un contrat *stand alone* est qu'il spécifie son domaine d'activité et l'étendue des garanties qu'il propose. On trouve souvent une proposition de produit d'assurance articulé en quatre promesses distinctes et complémentaires : détection du problème (1), mise en place d'action de réparation (2), puis identification de la source et protection pour éviter que cela se reproduise (3), enfin en parallèle à cela, une prise en charge de communication (obligation légale d'en informer les clients) (4). Il existe de nombreuses couvertures différentes possibles dans une police cyber comme par exemple les pertes de logiciels ou de données, la perte d'activité, ou encore les coûts de notification [31].

Le *silent cyber* : couverture de cyber ignorée

Le *silent cyber* (ou "cyber silencieux") est une spécificité de ce risque et fait parti des problématiques les plus importantes aujourd'hui pour les compagnies d'assurance. Il s'agit des responsabilités que l'entreprise supporte au titre d'une autre police. Donc sous-estime le risque et donc ne demande pas la prime correspondante. Nous reviendrons sur ce point dans la partie sur le *silent cyber* [32].

Cependant, la difficulté des compagnies d'assurance à se placer sur ce marché, et la réticence des entreprises à souscrire nous pousse à nous poser certaines questions. L'incapacité des professionnels à proposer un produit adapté (alors qu'il s'agit d'un marché pesant plusieurs milliards de dollars [15], et encore grandissant), les problèmes des modélisations traditionnelles obsolètes pour prédire les pertes face à ce danger, et l'impossibilité de développer des outils robustes montrent la difficulté d'assurer cette menace. Nous pouvons donc légitimement nous poser la problématique de l'assurabilité du risque cyber, et des caractéristiques qui en font un risque si complexe à modéliser.

31. Voir en annexe K l'ensemble des garanties proposées.
32. Voir partie 1.3 page 27, sur les expositions silencieuses.

2 Les challenges et points d'attention dans la modélisation du risque cyber

Le risque cyber dans sa définition est complexe. En effet, la menace informatique est extrêmement vaste : la diversité des dommages, l'absence de limites géographiques et temporelles, les connexions entre les organisations, les différentes origines possibles etc. en font un risque particulièrement délicat à modéliser. Les problématiques spécifiques à la modélisation du risque cyber font l'objet de cette première sous-partie.

2.1 Données indisponibles sur un risque évolutif

Le premier véritable défi dans la modélisation du risque cyber est l'absence de base de données. En effet, l'articulation spéciale des sinistres qui en découle rend très difficile son recensement, ce qui entraîne un manque de données historiques cohérentes requises pour se familiariser avec les retombées potentielles issues d'une attaque cyber. Les méthodes classiques s'appuient sur des statistiques de sinistralité, les actuaires analysent le passé, modélisent les évolutions et projettent le futur afin d'anticiper les coûts et les besoins en couvertures d'assurance. Ce contexte d'absence de données s'explique par la réticence des entreprises à communiquer sur les survenances de sinistres cyber et leurs conséquences, mais également par la difficulté que rencontrent ces dernières à diagnostiquer ces attaques : leurs sources, leurs déroulements, leurs durées, et leurs coûts. De plus, il n'existe pas officiellement aujourd'hui en France, un organisme chargé de la collecte et la diffusion des données du risque cyber. L'absence de partage d'information explique en partie la difficulté de la modélisation en assurance, et l'hétérogénéité des offres du marché.

D'autre part, la menace cyber est qualifiée d'évolutive dans le sens où elle change sans cesse. En effet, que ce soit dans ses sources, dans ses procédés ou encore dans ses conséquences, le risque évolue rapidement et radicalement. Nous observons une force d'adaptation des pirates aux systèmes de sécurité, et une augmentation des compétences et outils parallèle au développement des procédés de défenses informatiques. Ainsi, l'analyse de l'historique de sinistralité ne suffirait pas et pourrait même induire en erreur dans le calibrage d'une couverture d'assurance. Prévoir une protection pour un aléa changeant comme ce dernier en s'appuyant sur le passé résulterait à un échec, la menace sous-jacente n'étant plus la même. Donc les méthodes classiques seraient obsolètes, le risque étant trop évolutif.

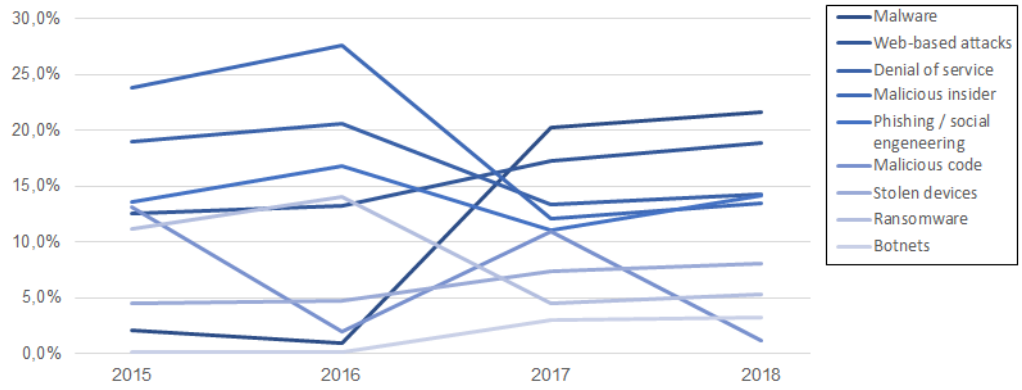


FIGURE 4 – Évolution annuelle des coûts des attaques cyber par type

Comme nous pouvons le constater sur la figure ci-dessus, extraite de la combinaison des rapports du Ponemon Institute 2017 et 2019 [33], le risque évolue énormément. Nous observons que les principaux types d'attaques varient en fonction des années, donc les couvertures assurantielles doivent s'adapter aux différentes tendances. Ainsi, l'évolutivité du risque cyber est une réalité et vient poser une nouvelle problématique dans la création d'offre d'assurance et dans la réalisation de modélisations.

2.2 L'exposition silencieuse

Au cours des dernières années, alors que le marché cyber continuait de croître et de se développer, il a été de plus en plus reconnu que les pertes liées aux attaques cyber ne se limitent pas au marché cyber spécifique ("*stand alone*"), mais peuvent également avoir une incidence sur les secteurs d'activités traditionnels. La sophistication croissante de la menace cyber et les pertes matérielles résultant d'évènements cyber récents tels que l'incident de NotPetya [34], qui a eu des répercussions sur les marchés de l'assurance dommages notamment, ont montré que des pertes importantes en termes de risque et de cumul résultant d'attaques cyber sont malheureusement possibles. Cette prise de conscience a renforcé l'attention du marché et de la réglementation sur le risque cyber "*silent*" et il existe désormais un consensus croissant sur le marché de la (ré)assurance, selon lequel cela doit être géré de manière appropriée [13].

Un risque cyber "silencieux" (ou non-affirmatif) (*"silent"*) désigne toute exposition au sein d'un programme d'assurance traditionnel susceptible de subir des pertes liées à des évènements d'origine informatique, car le risque cyber n'a pas été explicitement exclu de la police, sa formulation est sous-entendue ou incluse (gratuitement). En effet, l'apparition de sinistre cyber est probable, ce qui modifie l'équilibre des portefeuilles et biaise le calcul des primes par rapport aux pertes attendues avec une hausse de la fréquence des sinistres. Alors que la réalité du marché a changé, les assureurs

33. Source : "*Cost of Cyber Crime Study*", 2019 - Ponemon Institute, developped by Accenture.
34. Voir partie 1.2 page 19 sur les attaques historiques.

(et réassureurs) prennent de plus en plus de mesures pour quantifier, surveiller et soumettre à des tests de résistance les expositions non-affirmatives sur l'ensemble du portefeuille et, dans la mesure du possible, transférer ce risque. En effet, l'attention particulière (et croissante) du régulateur invite chacun des acteurs à déterminer si l'exposition existe, si elle est bien tarifée et en parallèle à vérifier que la sinistralité causée est bien identifiée. Cette prise de conscience progressive de l'augmentation de la fréquence des attaques et donc du poids de l'exposition cyber sur les portefeuilles de garanties pousse les assureurs à proposer des réponses : que ce soit des mises en place d'exclusions, des transferts en réassurance ou encore des sous-limitations ou des extensions cyber. On appelle ce processus "l'affirmation" de l'exposition silencieuse.

D'autre part, l'un des problèmes centraux est que, contrairement aux pertes cyber positives, les évènements "silent", en particulier ceux susceptibles de causer des dommages physiques, sont généralement confinés géographiquement. En conséquence, la plupart des scénarios développés sur le marché restent centrés sur les États-Unis (et dans une moindre mesure sur le Royaume-Uni), ce qui rend difficile toute conclusion pour les (ré)assureurs opérant en dehors de ces pays. En conséquence, un grand nombre d'assureurs qui n'exercent pas leurs activités dans cet espace sont sous-desservis par ce qui est actuellement disponible sur le marché. Cela est particulièrement vrai pour le marché français de l'assurance où, jusqu'ici, l'attention limitée portée par les fournisseurs de modèles et les régulateurs n'a laissé que très peu de scénarios aux assureurs pour quantifier les pertes potentielles dues au risque cyber. Pour combler ce manque, nous proposons dans ce mémoire un scénario créé pour la région Île-de-France.

L'enjeu d'affirmer son exposition (c'est-à-dire de la rendre *affirmative* : donc de l'identifier puis la quantifier) est particulièrement important. L'exposition silencieuse, même muette (ne générant pas de sinistre), est existante et s'accroît : la prise de conscience de son existence progresse, aussi bien que la fréquence des attaques augmente. D'autre part, l'exposition silencieuse est l'objet d'une attention toute particulière de la part du régulateur. L'EIOPA [35] souhaite connaître la faculté de chacun des acteurs à déterminer si l'exposition existe, si elle est bien tarifée et si les sinistres qui en résultent sont en effet identifiés. L'objectif étant d'obtenir une affirmation totale de l'exposition.

2.3 Risque d'accumulation

Le principe du risque d'accumulation est qu'un évènement peut avoir de nombreuses conséquences. C'est un phénomène connu, mais est d'autant plus vrai dans le cas du risque cyber. Prenons l'exemple des vulnérabilités 0-day : s'en servir pour un piratage revient à exploiter une faille qui n'a pas encore été comblée par les développeurs du logiciel, afin d'installer un logiciel malveillant sur le

35. *European Insurance and Occupational Pensions Authority* est l'autorité européenne des assurances et des pensions professionnelles (ex-CEIOPS depuis 2010). Il s'agit d'une des trois autorités européennes de surveillance du Système européen de supervision financière. Source : Wikipedia, 2019.

réseau. Prenons l'exemple d'une faille sur un logiciel comme Microsoft, le temps qu'elle soit découverte puis réparée par les experts en défense cyber, les pirates pourraient envahir de nombreuses machines. En effet, les entreprises et particuliers de mon portefeuille utilisant Microsoft comme système d'exploitation sont extrêmement nombreux, donc la même faille va être utilisée en boucle jusqu'à ce que la solution soit trouvée et la mise à jour soit effective. Nous voyons effectivement que la corrélation entre les expositions est grande et que les interconnexions des réseaux soulèvent une véritable problématique assurantielle. La figure ci-dessous illustre cette problématique des interconnexions.

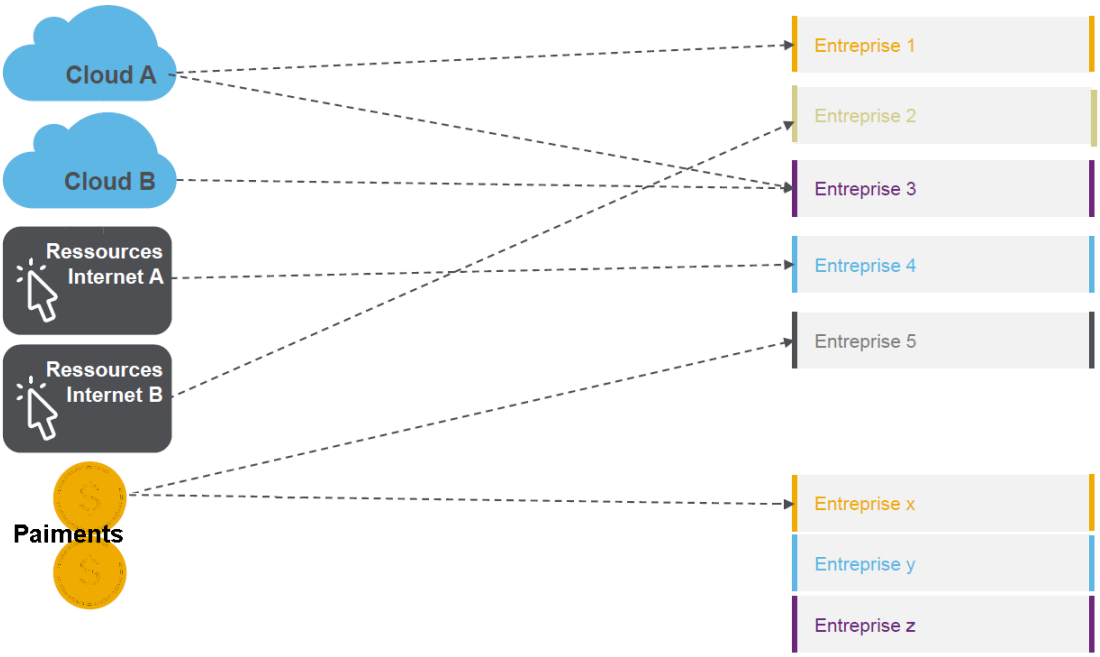


FIGURE 5 – Modélisation des sources de cumuls dans un portefeuille cyber

Cette figure représente les sources de cumuls au sein d'un portefeuille [36]. La modélisation des interconnexions et des sinistres résultant d'expositions silencieuses cyber est particulièrement délicate. Cependant, les acteurs du marché ont besoin d'imaginer des solutions à ce problème et donc d'avoir des estimations du risque supporté. La création de scénarios permet de mesurer l'exposition de son portefeuille au risque cyber, de prendre en compte les interconnexions et de toucher plusieurs polices.

36. Modélisation du risque Cyber, Q. Huin Morales & I. Hamny - Aon Reinsurance Solutions, 2019.

3 L'assurabilité du risque cyber

L'intérêt de l'analyse de l'assurabilité réside dans la réflexion sur la possibilité ou non de trouver un échange entre risque et prime qui soit socialement, légalement et mathématiquement équitable dans la durée. En particulier, cette allocation équilibrée devrait amoindrir les risques par diversification et mutualisation. En outre, le risque résiduel sera supporté par les acteurs qui ont une vocation de gestionnaire de risques : les assureurs, réassureurs et agents des marchés financiers. Les conséquences diverses des limites de l'assurabilité sont considérablement sous-estimées, nous allons étudier l'assurabilité du risque cyber en France dans cette section.

3.1 Qu'est-ce que l'assurabilité ?

L'assurabilité d'un risque est la capacité des agents à concevoir un produit d'assurance concret et opérationnel, précisément pour cette menace. Nous allons nous appuyer dans cette étude sur différents aspects de l'assurabilité d'un risque en nous basant notamment sur les travaux du docteur Baruch Berliner [37] [2]. Ce travail reprend la méthodologie et plusieurs résultats (mis à jour) d'une étude de l'Université de St. Gallen [3], en approfondissant certains axes de travail proposés, et en développant davantage les conclusions présentées.

Afin de pouvoir dire d'un risque qu'il est "assurable", ce dernier doit, d'après Berliner, correspondre à plusieurs conditions qui sont réparties en trois principales catégories, présentées dans le tableau ci-après.

Les critères d'assurabilité		**Exigences associées**
Sociétaux	(1) Politique publique	Conforme aux valeurs de société
	(2) Restrictions légales	Permettent la couverture
Marché	(3) Primes d'assurance	Suffit au recouvrement des coûts et abordable
	(4) Limites des couvertures	Acceptables
Actuariels	(5) Caractère aléatoire des pertes	Indépendance et prévisibilité de l'exposition
	(6) Perte maximum probable	Queue de distribution fine
	(7) Perte moyenne par évènement	Perte moyenne modérée
	(8) Exposition	L'exposition doit être importante (application de la loi des grands nombres)
	(9) Asymétrie d'information	Aléa moral et sélection adverse raisonnables

Table 2 – Les critères d'assurabilité d'un risque d'après Berliner (1982)

Notons cependant qu'il existe d'autres critères que nous n'avons pas énoncés dans le tableau ni

37. Dr Berliner est un économiste et artiste Israélien né en 1942, auteur de nombreux articles à caractère actuariel notamment "*Limits of insurability of risks*" en 1982.

dans le paragraphe précédent parce qu'ils n'ont pas d'intérêt particulier pour notre étude, et sont vérifiés immédiatement [38].

3.2 Analyse de l'assurabilité : critères de marché et impact sociétal

Nous allons dans un premier temps nous orienter vers l'explication des critères sociétaux puis les contraintes de marché avant de nous concentrer sur les critères actuariels. Ces premières explications seront donc plutôt qualitatives.

3.2.1 Critères sociétaux

Politique publique

L'apparition d'un nouveau produit d'assurance, ou la volonté d'en créer un, pour protéger d'un risque soulève plusieurs interrogations. Cela peut paraître contradictoire mais une telle couverture pourrait même rendre ces crimes plus attrayants : en effet, la fraude à l'assurance en serait encouragée, car les attaques informatiques de manière générale sont difficiles à détecter, mais également quasiment impossible à relier à leur source, à l'auteur.

D'autre part, les entreprises peuvent être moins incitées à se protéger elles-mêmes. Une protection adéquate élaborée est coûteuse et complexe à mettre en place. Ainsi, si elle se sait couverte pour ce type de risque, on peut considérer logique que les défenses vont s'en voir impactées. Or, la réduction de la sécurité informatique de ces entreprises augmenterait l'exposition globale au cyber et entraînerait ainsi des pertes plus importantes en termes financiers pour les assureurs mais surtout en termes de bien-être social. On se rappelle historiquement de nombreux scandales informatiques de pertes de données ayant résulté à des tragédies (comme par exemple au Canada, deux suicides suite au *DataBreach* du site de rencontre extra-conjugale *Ashley Madison*, en 2015 [39]) ou des violations de vie privée (*exp :* l'acteur Charlie Sheen contraint de révéler qu'il est positif au VIH après le *hack* de Sony Pictures, 2015). Ainsi, assurance et auto-protection se comportent comme des substituts, alors qu'ils sont en réalité des compléments.

Cependant, d'autres experts estiment que l'assurance augmenterait les investissements dans la protection informatique et générerait ainsi des issues positives [26]. En effet, le développement d'un produit d'assurance cyber implique également des normes et des conseils relatifs à la protection du réseau. Proposés par la compagnie d'assurance en charge, par le gouvernement ou même par le régulateur, ces pratiques conseillées permettraient donc à l'inverse, de réduire l'exposition. On observe déjà ce phénomène sur d'autres produits d'assurances (la plupart) : en MRH par exemple, le

38. Citons par exemple, le caractère "futur" que le risque doit avoir : il ne peut pas y avoir de rétroactivité dans une couverture d'assurance, ou encore le caractère "réel" du bien protégé.

39. *Ashley Madison : 'Suicides over website hack'*, C. Baraniuk - Technology reporter, 2015.

fait de posséder une alarme ou une porte à double verrou permet de faire baisser la prime d'assurance (car diminue la probabilité de se faire cambrioler), et donc incite l'assuré à investir dans ces systèmes de protection. On imagine la même situation dans le cas du risque cyber.

Les arguments que nous avons exposés précédemment nous invitent à penser que la protection des réseaux relève aussi bien du privé que du public, et donc que l'état devrait avoir un rôle à jouer, au même titre que les entreprises et les particuliers. En effet dans sa définition, le gouvernement est en charge de la protection des citoyens ainsi que du maintien de l'ordre. S'il s'agit d'un bien public, alors l'intervention de l'autorité publique est souhaitable, que ce soit dans la gestion de ce risque ou dans la protection des habitants du pays.

FIGURE 6 – Kit de sensibilisation de CYBERMALVEILLANCE.GOUV

Compte tenu des conclusions d'une influence positive de l'apparition d'une couverture d'une assurance cyber sur la sécurité numérique, une solution pour l'état pourrait consister à intervenir dans la promotion de ce marché. La sensibilisation, au même titre que pour la sécurité routière ou l'anti-tabagisme, pourrait être la mission des autorités françaises. L'image ci-dessus représente une première volonté de l'état dans ce sens. Il s'agit d'un kit gratuit mis à disposition par le site internet du gouvernement pour communiquer sur l'importance des risques numériques, transmettre les bonnes pratiques et de manière générale aider à améliorer l'hygiène informatique collective. On peut enfin penser à d'autres mécanismes dans lesquels on pourrait le voir intervenir :

- Couverture obligatoire en matière d'assurance cyber pour entreprises et particuliers ;
- Subvention pour l'auto-protection et l'investissement dans la sécurité numérique ;
- Intervention du gouvernement en tant qu'assureur de dernier recours : solution au manque de capacité de réassurance [8].

Les limites d'assurabilité ne sont donc pas trop importantes en terme de politique publique, bien que le critère ne soit pas tout à fait rempli.

Contraintes légales

L'assurabilité d'un risque peut être freinée par la loi. En effet, des restrictions légales pourraient empêcher certaines couvertures dans l'assurance cyber. Par exemple, dans de nombreux pays, il est interdit de se protéger contre les amendes réglementaires [16], il s'agit d'un véritable débat dans le cas du risque cyber, notamment avec les RGPD en vigueur depuis 2018. En outre, la législation en terme de protection des données et sur le risque cyber en général évolue assez rapidement en ce moment en Europe (et dans le monde), et donc les règles changent. Certains nouveaux systèmes pourrait faire apparaître des risques ou des restrictions supplémentaires qui pourraient donc bénéficier d'une couverture d'assurance. Par conséquent, le risque de modification de la réglementation et des lois est un problème important pour les assureurs dans le cadre du risque cyber. D'autre part, les conditions générales de la police d'assurance doivent être ajustées lorsque de nouvelles réglementations entrent en vigueur, mais peuvent en parallèle entraîner une demande nouvelle et importante d'assurance.

Enfin, la divulgation des informations nécessaires dès le départ (évaluation des risques) ainsi que pendant le contrat (inspections) pourrait poser problème du point de vue de la protection des données. Il est raisonnable d'admettre que certains établissement (de santé par exemple) pourraient ne pas accepter de partager leurs données à un tiers, même un assureur.

3.2.2 Critères de marché

Primes d'assurance

Les primes d'assurance ont pour objectif d'être suffisantes pour le recouvrement de la sinistralité transférée, et abordable pour l'assuré. Les coûts actuels des couvertures cyber sur le marché semblent ne pas être adaptés : certains les jugent trop chères, d'autres incohérentes. Il existe de nombreuses raisons pour expliquer cela : le produit est spécifique et le marché est très jeune, donc le risque n'est pas suffisamment mutualisé pour que le prix en soit significativement amoindri. De même, la concurrence n'est pas saturée donc les prestations restent chères. Une définition simple du critère de prime pour l'assurabilité d'un risque est l'existence des deux parties consentantes : s'il est possible de trouver deux agents prêts à effectuer un transfert de risque pour un montant spécifique.

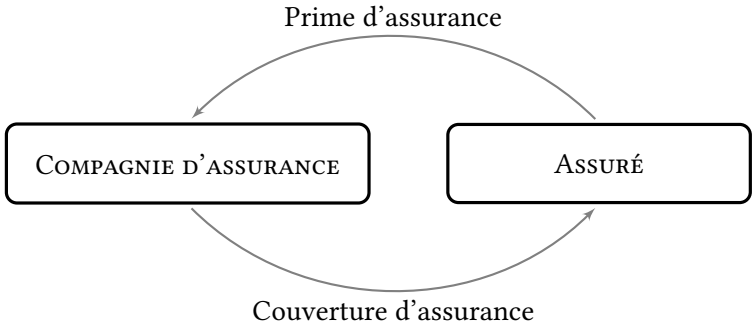


Figure 7 – Transfert de risque, principe de l'assurance

Cette volonté commune n'existe que si à la fois vendeur et acheteur y trouvent leur compte. Dans le cas du risque cyber, un tel échange n'est pas si évident. Enfin, la grande asymétrie d'information incite les assureurs à se montrer prudents. D'après Betterley, ce haut coût des protections dans le domaine de la cyber sécurité s'explique principalement par les importantes incertitudes impliquées. Les prix devraient finir par revenir au raisonnable et se stabiliser [25], comme on commence à le voir sur le marché américain, marché le plus mature (ou plutôt le moins immature) de la planète. Certaines études, notamment de l'institut de recherche Ponemon, expliquent pourquoi les prix des assurances cyber ne sont pas déraisonnablement élevés [20].

Ainsi, pour un risque comme le cyber, pouvant avoir un impact quasiment général (perte financière, de réputation, de temps, de client, d'exclusivité, ...) avec des variations très grandes (en fonction du temps, du secteur d'activité, de la région géographique, etc.), la détermination de la prime est particulièrement difficile, peu importe la méthode choisie. Nous pouvons malgré tout nuancer ce propos en affirmant (comme évoqué précédemment) que la prime d'assurance est un problème mais pas forcément très important parce que la seule véritable conséquence qu'il pourrait avoir est d'empêcher le transfert de risque, or ce n'est pas le cas pour le cyber. Tant qu'on trouve des acheteurs et des vendeurs prêts à effectuer cet échange, les primes d'assurance non-adaptées n'ont pas plus d'impact que du déficit pour l'assureur ou une réticence à souscrire pour l'assuré.

Limites des couvertures

Pour qu'un risque soit assurable, il faut pouvoir donner un maximum cohérent dans la prise en charge. Les plafonds de couverture d'assurance cyber sont relativement bas, bien qu'au vu de nos bases de données, ils semblent suffire pour les sinistres que nous avons recensés. La suffisance de ces plafonds dépend de l'appétence et de la politique de gestion du risque de l'entreprise en question. Les limites sont assez variables sur le marché français.

Cette complexité est un réel problème dans la détermination de la limite des couvertures pour (entre autres) les raisons suivantes :

- Beaucoup d'exclusions dans le cadre des assurances cyber : le terrorisme, les pertes dues à une erreur interne ("*self-inflicted loss*"), ou encore l'espionnage industriel (le "*spying*") font souvent l'objet de clauses d'exclusions ;
- La nature évolutive (historique obsolète) et complexe du risque lui-même (notamment la difficulté de le rattacher à sa source) ;
- Le *silent cyber* : les sinistres cyber n'atteignent pas seulement les polices cyber spécifiques. On peut avoir des dommages RC ou MRH par exemple ayant des origines cyber. On appelle cela le *silent cyber*[40] ;
- L'incertitude du vendeur et de l'acheteur de couverture ;
- Pertes difficilement mesurables[41].

Nous pouvons également insister sur les difficultés à savoir ce que couvrent les polices souscrites : le risque étant complexe, on ne sait pas quelle forme prendra le sinistre. L'ENISA présente cette incertitude comme l'une des raisons pour lesquelles les entreprises n'achètent pas d'assurance cyber [8].

Ainsi nous avons pu constater les limites de l'assurabilité du risque cyber en terme de critères de marché :

- Pour les primes d'assurances, bien que leur montant exact ne soit pas uniforme ni équitable pour les clients, tant que deux parties sont en accord pour procéder à l'échange entre le risque et la prime, la problématique n'est pas un frein au développement du marché assurantiel ;
- Les limites des couvertures sont difficilement mesurables et ne permettent pas l'existence d'une véritable protection d'assurance : l'exposition étant tellement grande (et difficile à mesurer) que l'équilibre du transfert de risque n'est pas possible, et les acteurs ne peuvent pas assumer une telle menace dans son intégralité.

3.3 L'assurabilité mathématique du risque cyber

Dans cette partie nous allons nous intéresser aux critères actuariels d'assurabilité du risque cyber. Pour pouvoir évaluer la validité de cet ensemble de conditions nous avons besoin de bases de données. Or, comme nous l'avons exprimé précédemment, le manque de données est problématique dans l'étude de ce domaine. Nous allons donc utiliser, comme C. Biener, M. Eling et J.H. Wirfs [3], une base de SAS de risque opérationnel : **SAS OpRisk Global Data**[42].

Cette base est constituée par SAS et recense des pertes opérationnelles. Cette dernière répertorie tout incident de montant supérieur à 1 000 000 USD, entre Mars 1971 et Juillet 2019. Ainsi, sont

40. ou "Cyber silencieux", voir partie 1.3.
41. Voir partie 1.2 page 21 sur les types de pertes.
42. *The data analysis for this paper was generated using SAS ®OpRisk Global Data. Copyright, SAS Institute Inc. Cary, NC, USA. All Rights Reserved.*

documentés plus de 35 000 événements dans tous les secteurs d'activité avec leurs caractéristiques. Notons que l'on entend ici comme risque opérationnel, toutes les incertitudes et les dangers auxquels une entreprise fait face lorsqu'elle exerce ses activités quotidiennes dans un secteur donné. Afin de séparer les incidents cyber des autres pertes, nous avons développé un algorithme de fouille de texte dans la description de chaque sinistre. Nous avons utilisé la même base de mots-clés que dans l'étude de l'université St Gallen.

Le principe de différenciation des incidents cyber est le suivant : on classifie en cyber tout incident ayant simultanément une cible numérique, un résultat de perte et un acteur informatique (humain, technique ou externe). En recherchant les mots clés dans les descriptions de la base SAS, nous pouvons effectuer une telle distinction [43].

Caractère aléatoire et indépendant des pertes

La conception mathématique actuarielle sur le problème d'aléa dans l'assurabilité est habituellement résumée en affirmant qu'un risque est assurable si la Loi des Grands Nombres (LGN) peut s'appliquer. D'autre part, le caractère incertain du risque cyber est problématique puisque l'inconnue aléatoire n'est pas sur la probabilité ou non d'être attaqué mais sur la vulnérabilité de l'entreprise, sa capacité à se protéger, ce qui n'est pas vraiment aléatoire.

En effet, l'étude de corrélation des risques est importante dans le cadre de l'assurance, puisqu'elle détermine le risque de cumul. C'est pourquoi il existe des méthodes pour lutter contre ce risque résiduel comme la diversification du portefeuille ou la réassurance par exemple. Cette condition semble problématique dans le cas de la menace informatique. En effet, on peut notamment attester qu'aujourd'hui, les réseaux sont très partagés : il s'agit du problème de l'interconnexion et des risques d'accumulation évoqués précédemment. On peut donc remettre en cause l'indépendance supposée des menaces cyber entre les différentes entreprises [44], ce qui limite le cadre d'application de la loi des grandes nombres.

Alors que les entreprises se soucient de la défaillance corrélée des systèmes au sein de leur propre réseau (corrélation interne) qui se traduit en un sinistre individuel élevé pour une compagnie d'assurance, qui donc s'inquiète plutôt de la corrélation globale dans l'ensemble de son portefeuille qui grossit le cumul. Ci-dessous sont présentés quelques exemples de ces corrélations [4].

43. Les détails sur ces travaux sont décrit en annexe L : "Analyse statistique de la base SAS".
44. Haas and Hofmann (2013), Hofmann and Ramaj (2011), Raghunathan, Ögüt, and Menon (2011), Bolot and Lelarge (2009).

	Corrélation globale ρ_G	
Corrélation interne ρ_i	Faible	Forte
Forte	Attaque interne / Sabotage	Vers et Virus
Faible	Echec de logiciel	Logiciel espion / *phishing*

Table 3 – Exemple de corrélations pour différents risques informatiques

D'autre part, une entrave au caractère aléatoire des pertes est l'implication forte du régulateur. En effet, la possibilité d'une intervention réglementaire massive modifiant les règles applicables pour assurer ces pertes est une contrainte pour l'hypothèse d'aléa. Il s'agit ici de modifications qui entraîneraient la présence de nouveaux risques et l'obligation d'une adaptation de la stratégie de gestion des risques des entreprises.

Ce critère pose plusieurs véritables problèmes de fond : d'une part, les corrélations entre les risques et les expositions des entreprises viennent perturber le caractère aléatoire et indépendant d'un risque assurable. D'autre part, la diversification en semble donc considérablement amoindrie et surtout très difficile à mettre en place. Enfin, le manque d'information sur la nature même du risque (et son caractère complexe et évolutif) et de base de données pour l'étudier rend délicat son assurabilité.

Perte maximum probable

Dans le cas d'un risque assurable, les pertes maximales doivent être peu probables. En effet, l'étude des distributions de ces pertes doivent montrer une queue fine. Pour les menaces avec un historique conséquent, la théorie des valeurs extrêmes permet d'obtenir une distribution probabiliste sur l'interpolation des queues (valeurs extrêmes) de variable aléatoires expérimentales : ici les montants des pertes cyber.

Ces approches théoriques (TVE) ne sont pas adaptées dans le cadre de notre étude par difficulté à paramétrer des lois sur des données trop peu disponibles. Ici nous pourrions estimer que la perte maximum probable doit être gérable pour une compagnie d'assurance dans le cadre du risque cyber afin que ce critère soit validé.

Type de sinistre	**Montant max. de la perte (en m USD)**
cyber	5 478,0
non-cyber	5 483,0

Table 4 – Montant maximum des pertes cyber vs non-cyber

On peut donc simplement comparer les maximums des sinistres cyber et non-cyber de la base de données sur le tableau précédent.

Or, les limites des couvertures protègent les assureurs dans tous les cas. Donc les pertes maximales probables ne sont a priori pas un problème. Nous pouvons tout de même soulever le problème que ce sont les limites d'assurance qui définissent la perte maximum pour l'assureur. Mais pour l'entreprise, la perte maximum probable est quasiment infinie. On peut donc assez logiquement imaginer que le risque maximum porté par une entreprise est la perte totale de ses actifs, de ses clients, de son activité. Les pertes sont particulièrement hétérogènes dans la menace informatique, et les sinistralités maximales peuvent être très élevées pour les entreprises, et ce malgré une couverture assurantielle cyber.

Ce critère n'est donc pas profondément problématique pour les assureurs qui peuvent se protéger avec des limites, des processus d'affirmation et du transfert de risque à la réassurance. Si nous sortons du cadre de l'étude de cette base de données, nous avons vu par l'historique que certaines agressions cyber ont eu des conséquences immenses, de plusieurs millions voire milliards d'euros de pertes. On peut légitimement estimer que cela est problématique, le marché n'a pas (encore) les capacités pour absorber de tels montants.

Perte moyenne par évènement

Pour pouvoir comparer les pertes moyennes par évènement et ainsi observer de manière optimale les différences de nature entre ces deux types de sinistres, le diagramme *boxplot* semble le plus adapté. En effet, comme nous pouvons l'observer ci-dessous, il illustre plusieurs points clés de notre analyse. [45] On observe illustrées sur la figure ci-dessous les moyennes du tableau récapitulatif.

Type de sinistre	Montant moy. de la perte (en m USD)	Ecart-type (en m USD)
cyber	1 662,9	1 725,9
non-cyber	1 853,9	1 717,9

Table 5 – Comparaison des coûts moyens de sinistres cyber et non-cyber

On peut voir que la moyenne du prix par évènement pour les incidents cyber est inférieure à celle des dégâts causés par des sinistres non-cyber. Nous pouvons en revanche noter que l'écart type est légèrement supérieur dans le cas du risque cyber, donc plus de volatilité. Mais nous restons dans le même ordre de grandeur. Ainsi, on peut considérer ce critère rempli après étude de notre base de données. : il ne semble pas soulever d'interrogation particulière.

Exposition

Nous avons déjà discuté de l'hypothèse problématique des corrélations, mais on peut ajouter à cette dernière dans le cadre de la modélisation du risque cyber le fait que les échantillons pour la

45. Dans un *boxplot* classique la médiane est affichée (ici en noire). Pour le bien de cette étude nous avons également affiché dans R la moyenne (en couleur sur le graphique).

diversification dans les portefeuilles d'assurance sont relativement faibles. En effet, les entreprises et particuliers qui souscrivent à des assurances cyber sont encore assez peu nombreux. Alors même si en effet l'exposition au risque cyber est très importante, comme nous l'avons répété plusieurs fois dans cette étude, les assureurs doivent s'efforcer de trouver plus d'assurés afin de bien diversifier leurs risques. On peut ajouter également que l'exposition au risque cyber dépend grandement de la taille de l'entreprise, mais aussi de son secteur d'activité.

Asymétrie d'information

La matière première du marché de l'assurance est le transfert de risque. Il se trouve que lors de cet échange de prime d'assurance contre une protection, les deux acteurs n'ont pas forcément accès aux mêmes informations. On appelle cela l'asymétrie d'information. Ce phénomène est particulièrement problématique dans le cas du risque cyber, et peut aboutir à une sélection adverse (également appelée anti-sélection) ou à un aléa moral. Ces derniers permettent d'expliquer parfois pourquoi des marchés d'assurance concurrentiels échouent à fournir un niveau d'assurance efficace. L'asymétrie d'information atteint les prix, la qualité, les composants (etc) de la grande majorité des marchés.

L'aléa moral résulte de l'absence d'incitation de l'assuré à prendre des mesures de protection personnelle qui réduiraient la probabilité de perte ou l'ampleur d'une perte une fois qu'il s'est produit suite à l'achat d'une assurance. C'est-à-dire, une baisse des dépenses en cyber sécurité lorsque l'on souscrit à une assurance. L'unité du réseau et les ressemblances entre les connexions des entreprises impliquent que la réticence à investir d'une firme peut handicaper toutes les autres. Ainsi naît un problème de coordination. On appelle cela l'interconnexion (ou "inter-corrélation" [21]), il s'agit de l'observation selon laquelle les risques cyber des entreprises sont corrélés. Nous pouvons également voir cette problématique d'un autre oeil : une entreprise qui se protège, protège également indirectement toutes les autres. Cela créé un rejet à vouloir investir dans la cyber sécurité. Pour lutter contre ce problème, les solutions classiques d'assurance peuvent être imaginées (comme un système bonus / malus sur les primes, l'apparition de franchise, ou encore l'imposition d'audit de système d'information).

Le problème de l'asymétrie d'information se révèle donc lui aussi vraiment problématique dans notre étude d'assurabilité. L'aspect théorique qui se confronte à un aléa moral trop important nous invite à penser que ce critère n'est pas complètement rempli. De même que pour la sélection adverse, où on comprend que le biais est trop grand pour être estimé négligeable. Le modèle assurantiel classique fonctionne pour une population d'individus certes hétérogène, mais ayant une connaissance commune innée sur le risque supporté et transféré [23]. Le problème de la sélection adverse entraîne une méconnaissance quasi-totale de l'exposition cyber des entreprises pour une compagnie d'assurance, et ainsi, l'assurabilité est vraiment remise en question.

Limites et conclusions sur l'assurabilité

Nous avons donc vu dans cette sous-partie plusieurs réponses aux critères proposés par Berliner [46]. Nous allons ici résumer ce qui a été évoqué avant d'en exposer les limites et les conclusions que l'on peut en tirer.

D'une part, en ce qui concerne les critères sociétaux de **politique publique** ou de **contraintes légales**, nous avons vu que les critères étaient relativement bien remplis. Nous pouvons tout de même émettre quelques réserves sur l'aléa moral et les fraudes, ainsi que les vides juridiques et les clauses de législation en vigueur qui pourraient perturber l'équilibre, mais ces problématiques seraient résolues avec le gain en maturité d'un tel marché.

D'autre part, à propos des **critères de marché** : les primes d'assurances et les limites de garanties présentent plus de contraintes. Pour les **primes d'assurance**, le principe est simple : le transfert d'un risque contre une rémunération. Malgré le faible nombre d'acteurs en place sur le marché et la grande variation des montants, les primes finissent par s'équilibrer avec la maturation du marché et le développement de la concurrence. En revanche pour les **limites des garanties**, nous avons un véritable dilemme : les assureurs se protègent pour l'instant par des limites acceptables et des exclusions, mais les coûts indirects de l'assurance cyber, les couvertures silencieuses et l'évolutivité du risque sous-jacent ne sont pas gérables pour le marché assurantiel. La gestion des limites des polices est donc une vraie problématique pour l'assurabilité de ce risque.

Enfin, les **critères actuariels** ont fait l'objet d'une étude plus quantitative. Nous pouvons déjà ainsi dire que les critères démontrés ici ne le sont en réalité que pour le risque opérationnel cyber (qui est a priori représentatif du marché). Avec la croissance des fréquences des évènements cyber et les différents types de risque cyber, l'**exposition** n'est pas problématique. La **perte maximum** non plus, comme nous l'avons vu précédemment, les assureurs se protègent par des limites de garanties et des exclusions. Enfin, la **perte moyenne par évènement**, qui devait être modérée, ne pose pas non plus de soucis (comme on peut le voir sur les *boxplots* précédents). En revanche, l'**asymétrie d'information** créé un véritable biais. Que ce soit l'aléa moral ou la sélection adverse, les conséquences sont trop grandes pour être négligeables. In fine, en ce qui concerne le caractère aléatoire des pertes, nous pouvons citer trois freins à l'assurabilité : d'une part, les corrélations trop élevées entre les risques, donc le manque de diversification possible dans ce domaine. D'autre part, le manque de données, qui empêche l'étude approfondie du comportement de ce risque. Et enfin, le caractère complexe et évolutif de la menace cyber.

Le tableau ci-dessous résume visuellement les résultats énoncés dans cette conclusion.

46. Voir tableau 2 page 32 sur les critères d'assurabilité.

Les critères d'assurabilité		Exigences associées	
Sociétaux	(1) Politique publique	Conforme aux valeurs de société	
	(2) Restrictions légales	Permettent la couverture	
Marché	(3) Primes d'assurance	Suffit au recouvrement des coûts et abordable	
	(4) Limites des couvertures	Acceptable	
Actuariels	(5) Caractère aléatoire des pertes	Indépendance et prévisibilité de l'exposition.	
	(6) Perte maximum probable	Queue de distribution fine	
	(7) Perte moyenne par évènement	Perte moyenne modérée	
	(8) Exposition	L'exposition doit être importante (application de la loi des grands nombres)	
	(9) Asymétrie d'information	Aléa moral et sélection adverse raisonnables	

TABLE 6 – Vérification des critères d'assurabilité

La conclusion à tirer de cette étude est la suivante : les critères respectés parmi les conditions d'assurabilité permettent de proposer une couverture. En effet, le fait qu'il n'y ait pas de restriction légale, pas d'opposition en terme de politique publique, et qu'on puisse trouver des primes d'assurance qui sont acceptées par les deux partis lors du transfert de risque, rend possible l'existence de polices cyber. Ainsi, par la simple loi de l'offre et de la demande, il suffit qu'il y ait une volonté de se protéger contre la menace informatique via le marché assurantiel, et un intérêt pour les assureurs à se placer pour que l'on voit apparaître des produits de transfert de risque. Ceci explique pourquoi, malgré les limites de l'assurabilité évoquées, nous pouvons trouver des acheteurs et des vendeurs d'assurance cyber spécifique. En revanche, les problématiques soulevées ne disparaissent pas avec l'offre et la demande : l'asymétrie d'information et le manque d'indépendance et d'aléa identifiés pour ce risque empêche les produits d'assurance proposés d'être véritablement appropriés pour la protection du cyber, et les modélisations classiques de fonctionner. Le point positif que l'on peut tirer de cette conclusion et de l'étude de l'assurabilité du risque cyber est que les limites à l'assurabilité sont principalement dues à la jeunesse du marché et se verront résolues avec l'approfondissement de la connaissance en ce domaine.

Deuxième partie

Mesure du risque cyber : constructions de modèles & hypothèses

4 Présentation du portefeuille

4.1 Construction du portefeuille

Les informations dont nous disposons dépendent de l'entreprise Aon France qui nous laisse les exploiter pour le bien de ce travail de recherche.

La base de données initiale est un portefeuille de couverture d'un client pour une assurance cyber qui englobe plusieurs polices (RCP [47], dommages aux biens, perte d'exploitation, vol ou perte de données, garantie de gestion de crise ...) que nous avons complété avec d'autres couvertures plus classiques. Il est extrait des bases client de 2019. Nous disposons de plusieurs renseignements par engagements, fournis par la cédante. La sous-partie suivante, de statistiques descriptives, a pour objectif de fournir une analyse détaillée de la composition du portefeuille. Nous disposons ici principalement de deux catégories d'informations :

- Des données précises sur l'entreprise assurée : son identification (nom, numéro ID), sa position géographique (région, pays, ...), son secteur d'activité, son chiffre d'affaire annuel, son nombre d'employés, etc ;
- Des renseignements sur le contrat d'assurance : garanties souscrites, montant de la franchise, limite de la couverture, etc.

Notre position est d'estimer le risque de cumul pour une compagnie d'assurance, c'est une vision qui se rapproche du travail de la cession en réassurance. L'ambition de cette étude est double : la modélisation du cyber doit d'une part mesurer l'exposition au cyber des polices spécifiques et donc tarifer un risque pris en charge, et d'autre part couvrir l'éventuelle sinistralité causée par le cyber sur d'autres polices (comme la RCP ou bien la garantie perte d'exploitation) appelée les pertes silencieuses. Nous travaillons donc sur un portefeuille possédant plusieurs type de garanties, et pas uniquement du cyber.

4.2 Étude statistique du portefeuille

Nous allons présenter quelques statistiques descriptives afin de mieux saisir la composition du portefeuille dans son ensemble. Il convient de noter que ce portefeuille a été particulièrement

47. Responsabilité civile professionnelle.

construit pour notre étude, pour les modèles en question et les évènements imaginés (plus précisément pour le scénario "BO Île-de-France").En effet, le portefeuille choisi représente des couvertures (quasiment) exclusivement (99.7%) françaises. Plus précisément, comme nous le remarquons dans le tableau suivant, il s'agit d'assurés localisés en Île-de-France.

Ile-de-France	41 951 (84%)
Autre	8 049 (16%)

Table 7 – Répartition par région en nombre de lignes

Nous avons regroupé les régions hors Île-de-France, parce que ce qui nous intéressera est binaire : dans l'Île-de-France ou en dehors. Il est donc intéressant de remarquer que ce portefeuille est constitué à $83,9\%$ de police concernant un assuré en Île-de-France. En ce qui concerne plus précisément les entreprises qui constituent cet ensemble de police, on peut s'intéresser à la répartition par secteur d'activité (très utile notamment pour le modèle "fréquence $\times$ coût").

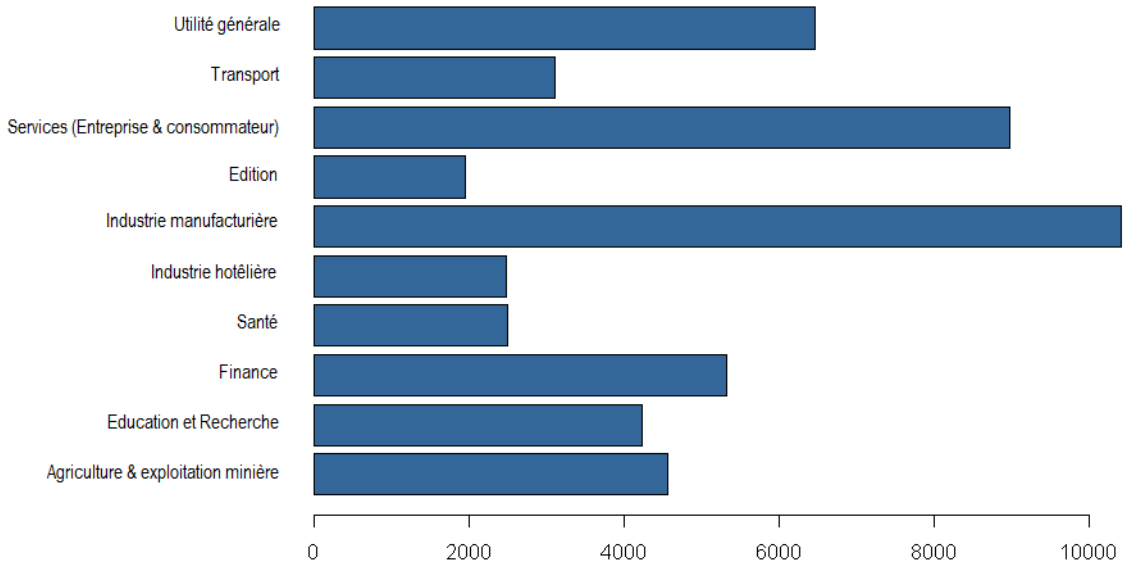


Figure 8 – Répartition des entreprises du portefeuille par secteur d'activité

Nous voyons qu'une grande diversité de secteurs d'activité sont représentés dans notre portefeuille.Une autre répartition à un degré plus grossier nous intéressera pour notre modèle par scénario, il s'agit des regroupements suivant :

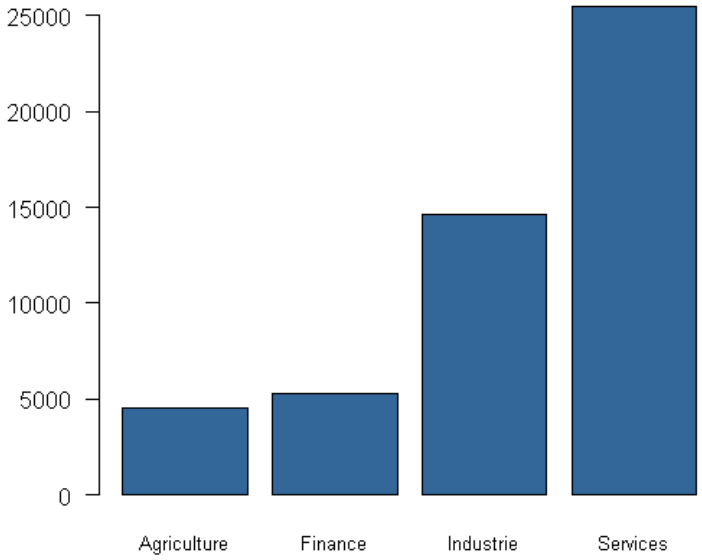


FIGURE 9 – Graphique de répartition par secteur d'activité (en nombre de lignes)

On compte dans le domaine d'activité des services, principalement le "service aux entreprises", terme employé pour les activité de prestations immatérielles (comme les activités comptables, juridiques, ou encore campagnes de publicités, ...) ou bien pour la performance (par exemple la maintenance, logistique, sécurité, ...) [48]. En ce qui concerne l'industrie, on considère ici les biens de consommation, d'équipement et autres biens intermédiaires. On y inclut également la construction, l'énergie, l'automobile et enfin l'agro-alimentaire. Cette organisation est supposée refléter l'ensemble du secteur afin d'exploiter ces informations dans nos modélisations.

Intéressons nous à présent à la répartition en terme de chiffre d'affaire des entreprises de notre portefeuille.

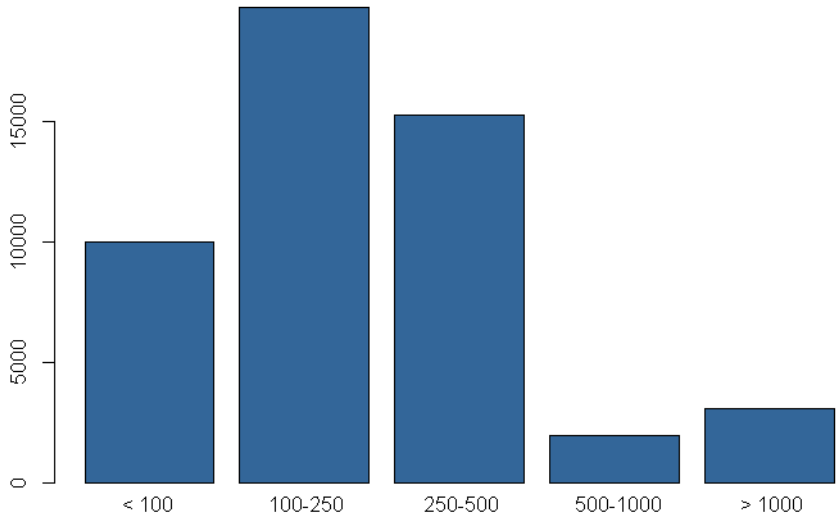


FIGURE 10 – Histogramme par tranche de chiffre d'affaire (en k EUR, par nombre de lignes)

48. Source : Direction générale des entreprises, 2019.

On remarque sur la figure précédente que les entreprises du portefeuille se répartissent en terme de chiffre d'affaire (CA) de manière assez hétérogène. C'est un atout pour notre modélisation. En effet, cela permet de voir le comportement du risque cyber sur des petites entités et sur des acteurs plus importants du marché. Enfin, le tableau ci-dessous donne plus de précisions sur la répartition des entreprises dans notre portefeuille en terme de CA.

	Minimum	Q. 25%	Médiane	Moyenne	Q. 75%	Maximum
CA Annuel	60 000	110 000	181 100	306 100	365 400	3 972 000

TABLE 8 – Répartition du chiffre d'affaire annuel

Nous pouvons à présent nous pencher sur la répartition de ces entreprises en terme de nombres d'employés. Cela sera un facteur important pour le second modèle, qui suit une méthode "fréquence $\times$ coût" dont les paramètres sont basés notamment sur la taille de l'entreprise en nombre d'employés. Nous avons fait le choix de présenter nos entités selon la classification internationale en fonction du nombre d'employés : Les TPE (Très petites entreprises, moins de 10 employés), les PME (Petites et moyennes entreprises, de 10 à 249 employés), les ETI (Entreprises de taille intermédiaire, de 250 à 4 999 employés) et enfin les GE (Grandes entreprises, plus de 5 000 employés). Ci-dessous, un graphique en secteur nous permet d'avoir un aperçu de cette répartition.

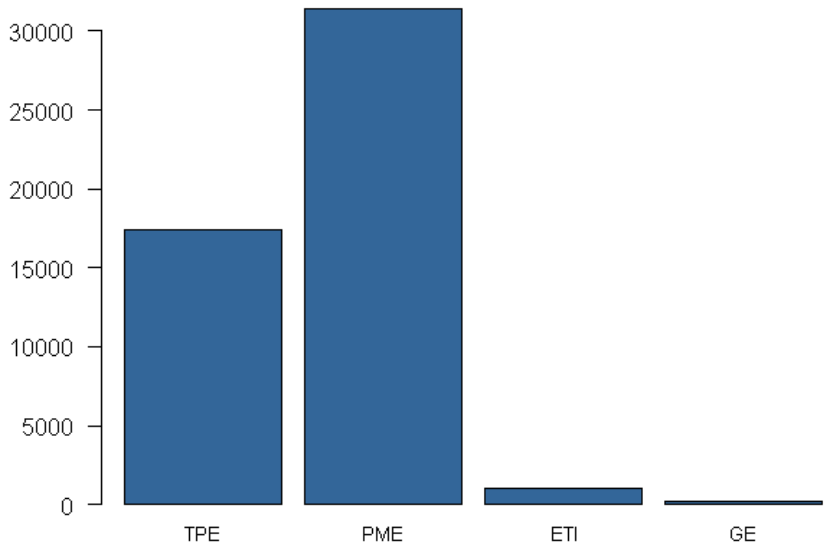


FIGURE 11 – Répartition des entreprises du portefeuille par nombre d'employés

Après s'être penché sur la composition du portefeuille en terme d'entreprises assurées, voyons à présent les programmes d'assurances de ces dernières. Relevons tout d'abord le fait que l'intégralité de ces engagements sont couverts pour les polices suivantes :

- RCP : Responsabilité civile professionnelle : couvre tout préjudice causé à autrui dans le cadre de l'activité de l'entreprise. Ici, si le préjudice en question est consécutif à une intrusion informatique ;

- Dommages aux biens : Comme son nom l'indique, il s'agit d'une garantie pour la détérioration de matériel ;
- "BI" : *Business interruption*, perte d'exploitation. La cessation d'activité causée par une source cyber ;
- "Data and software loss" : le vol ou la perte de données/de logiciels/d'outils ayant une origine informatique.
- Gestion de crise : déclenchement de cellule d'urgence et développement de techniques mises en oeuvre pour répondre à une situation de crise et en atténuer les conséquences.

Remarquons que certaines de ces polices sont spécifiquement orientées pour le cyber et d'autres en semblent, à l'inverse, décorrélées. Nous verrons pourtant que ces couvertures engendrent également de la sinistralité cyber. Voyons résumées ci-dessous les limites de ces couvertures. Notons que de nombreuses offres sur le marché demandent des franchises. Nous avons fait le choix de modéliser les pertes assurantielles sans franchise pour une meilleure visibilité. Cependant, le risque étant nouveau, il serait inapproprié de ne pas avoir de limite.

Limites	250 000 EUR	750 000 EUR
Effectif (nb. lignes)	21 459 (43%)	28 541 (57%)

TABLE 9 – Résumé des limites d'assurances du portefeuille

Nous avons ainsi analysé par des statistiques descriptives la composition de notre portefeuille, et nous allons à présent pouvoir expliciter la mise en place de la modélisation cyber.

4.3 Description des différentes approches

Le chapitre suivant à pour but de présenter la construction de plusieurs méthodes utilisées pour modéliser le risque cyber, les idées sous-jacentes ainsi que leurs limites. Nous allons également appliquer ces modèles à un portefeuille adapté du marché et ainsi estimer le risque supporté par les compagnies engagées. La modélisation du risque cyber est certainement l'un des challenges les plus complexes auquel font face les actuaires en ce moment. Certains outils se développent, proposant des approches nouvelles ou des méthodes historiques révisées. Nous travaillerons dans un premier temps sur la création d'un scénario spécifique au marché français, avant de nous pencher sur un modèle "fréquence $\times$ coût" (relativement "classique" en actuariat). Enfin, nous présenterons une approche nouvelle qui vise à mieux prendre en compte les spécificités du risque informatique, notamment les mesures de l'interconnexion. Nous présenterons les hypothèses, la théorie utilisée mais également les limites de ces différents modèles.

Les méthodes qui existent sur le marché aujourd'hui faillissent à prendre en compte entièrement les caractéristiques particulière de cette menace. Les problématiques principales du risque cyber que l'on retrouve dans les modélisations existantes sont les suivantes :

- Le manque de données et la difficulté de s'en procurer. Que ce soit pour les entreprises ou pour les compagnies d'assurances, il est très difficile de mesurer son exposition, d'analyser ses pertes et ses failles ;
- Les différentes origines possibles et la difficulté de remonter à la source de la faille informatique responsable du dommage cyber ;
- La diversité des sinistres et le large éventail des types de pertes possibles ;
- L'absence de confinement géographique, de limite physique des pertes matérielles ;
- L'absence également de limite temporelle à l'intrusion. Cette dernière peut rester muette pendant des mois, être détectée longtemps après le début des pertes ;
- Et enfin, les risques de corrélations entre les établissements et les violations.

Nous avons commencé par la présentation d'un portefeuille de garanties diverses auquel nous appliquerons ensuite les différentes modélisations que nous aurons construites pour l'appréhension du risque cyber.

5 La modélisation par scénario

5.1 Présentation du "Black-out Île-de-France"

Le point de vue adopté par certains acteurs du marché pour la mesurer l'exposition des couvertures d'assurances pour le risque d'accumulation cyber repose sur la définition d'évènements : cette approche consiste à créer un scénario pertinent, adapté aux caractéristiques (géographiques, garanties couvertes, secteurs d'activité, ...) du portefeuille étudié et à quantifier l'impact de ce dernier. Ainsi cette section a pour vocation de présenter les pertes consécutives à une attaque globale et coordonnée sur l'ensemble du réseau de transport et distribution (T&D) de l'entreprise Électricité de France (EDF), dans la région Île-de-France.

Pourquoi étudier un scénario Black-out en Île-de-France ?

Historiquement, pour étudier un risque nouveau sur un portefeuille d'engagements assurantiels, la méthode la plus simple est l'approche par évènement. Elle consiste en la création d'un scénario et en son application afin de quantifier l'exposition du portefeuille. En ce qui concerne le risque cyber, Lloyd's [49] a créé ce scénario en 2015 qui est devenu la véritable référence dans le calcul des couvertures d'assurance et de réassurance. Il s'agit donc du seul point de repère pour le placement, mais n'est pas calibré pour le marché européen.

Le manque de modélisation adaptée au marché français est un frein dans le développement et le calcul de couvertures assurantielles. Ainsi, cette étude vise à remédier à ce manque. Le scénario de panne du réseau de distribution d'énergie, également appelé "*Black-out Île-de-France*", est créé prudent et doit être considéré comme un sinistre catastrophique qui déclenchera plusieurs lignes d'assurance en Île-de-France et dans les environs.

Par conséquent, cette section décrit un évènement extrême mais plausible, ciblant le réseau électrique français, ainsi que les paramètres de calcul des pertes, assurantielles ou non, qui en découlent.

Résumé de l'étude

La section suivante décrit une attaque détaillée ciblant les principales sous-stations et les lignes de transmission qui alimentent les foyers et les entreprises. Cette dernière endommage physiquement les sous-stations de transport et les lignes électriques clés, dont la réparation prend du temps. En conséquence, l'évènement provoque des pannes importantes dans la région Île-de-France, distribuée par EDF, laissant une partie importante de la population sans électricité. A noter que cette région inclut notamment la capitale française, Paris, et accueille plus de 12 millions de personnes,

49. Nous nous référons dans ce mémoire aux *Lloyd's of London* en écrivant "Lloyd's" pour alléger le propos.

soit environ 19% de la population de France métropolitaine. Dans ce scénario, un logiciel malveillant est utilisé pour infiltrer le réseau EDF. À partir de là, les pirates sont en mesure d'identifier les faiblesses des systèmes de contrôles industriels à exploiter. Cela leur permet alors de cibler des zones sensibles du réseau et de communiquer directement avec les sous-stations.

Cet évènement entraîne des pertes d'assurance considérables dans tous les domaines, avec une attention particulière pour les pertes découlant de l'interruption éventuelle des activités (perte d'exploitation -PE-), car les entreprises dépendantes de l'approvisionnement en électricité ne peuvent fonctionner et les fournisseurs ne parviennent pas à livrer aux entreprises françaises, ce qui a un impact sur les principales chaînes de transmission. Le scénario et le rapport décrivent les actions d'acteurs sophistiqués forts de ressources techniques et financières nécessaires pour mener un assaut d'une telle envergure.

Cette situation doit être considérée comme extrême, mais elle souligne l'importance de la protection cyber des infrastructures nationales notamment sur des ressources essentielles.

Présentation de l'entreprise EDF

EDF

L'entreprise de production et de distribution d'énergie Française, **EDF**[50], est le premier fournisseur d'électricité en France métropolitaine. Le quasi-monopole d'EDF sur le sol français est un point négatif dans le cas de l'exposition au cyber parce que le risque d'accumulation est amplifié. Nous allons concentrer le travail de scénario sur la région la plus active du pays : dans ce cas, il est intéressant de noter que l'Île-de-France représente quasiment 4,5% du produit intérieur brut (PIB) de l'union européenne, et environ 31% du PIB Français (en 2012)[51].

Transmission et Distribution (T&D)

Afin de fournir ses clients, EDF s'appuie sur un réseau de lignes de transmission et de distribution (T&D) pour connecter l'électricité à partir des (très nombreuses) installations de production. L'épine dorsale du réseau T&D est constituée d'une série de lignes de transport de 500 kV (et 1MV) qui entourent l'Île-de-France. Le réseau T&D a pour fonction de déplacer l'électricité en veillant à un équilibre entre l'offre et la demande. Les activités de T&D relèvent des gestionnaires indépendants de transport (RTE) pour la HT (haute tension) et THT (très haute tension) et de distribution (Enedis) pour la moyenne et basse tension, dont la mission est d'assurer un accès continu aux réseaux. Ainsi, un potentiel pirate qui souhaiterait endommager le réseau de distribution d'énergie devrait forcément synchroniser son attaque sur plusieurs sous-stations de transmission en simultané pour pouvoir contourner les contrôles de sécurité.

50. "Electricité de France", créée en 1946.
51. Source : EuroStat, 2005.

5.2 Scénario d'une attaque cyber : les attaquants et l'infiltration

Les motivations pour attaquer l'Île-de-France

Une attaque de cette ampleur nécessiterait beaucoup de temps, de ressources et d'impunité d'arrestation (liberté de jouer avec les limites de l'informatique sans éveiller les soupçons) pour mener à bien l'ensemble des étapes nécessaires à la destruction du réseau. En conséquence, il est intéressant d'examiner les motivations des groupes à mener une telle entreprise, et examiner quels profils seraient les plus à même d'y parvenir. Pour ce faire, nous utilisons le travail précédent [52] de catégorisation des motivations des agressions cyber. Pour rappel, nous formons quatre familles principales : espionnage, idéologique, financier et destructeur. Cela nous permet d'identifier les capacités des groupes impliqués et de réduire en conséquence la portée de l'analyse.

- **Espionnage -** Le but principal de l'espionnage est de surveiller et de connaître un système sans se faire repérer. Comme ce scénario est conçu pour avoir un impact matériel sur des composants clés de l'économie française, il est peu probable que ce soit la motivation ;
- **Idéologique -** Les groupes hacktivistes ayant une motivation idéologique pour s'en prendre à la France pourraient être incités à mener une attaque. Cependant, jusqu'à présent, aucun groupe hacktiviste n'a montré qu'il avait les capacités ou le désir d'entreprendre un piratage de cette envergure. Cela ne veut pas dire que d'autres acteurs, tels que les États-nations, ne pourraient être motivés par des moyens idéologiques. Nous avons vu cela avec un certain nombre d'attaques russes contre l'Estonie et l'Ukraine en raison de leur relations historiques de l'époque soviétique [19] ;
- **Pécuniaire -** Dans ce cas, les motivations financières seraient difficiles à discerner. La perturbation elle-même causerait une perte économique à l'économie française et à EDF et RTE, mais il est difficile de déterminer comment la monétiser, si ce n'est miser sur les marchés boursiers pour parier contre les sociétés françaises et tirer profit des fluctuations des actions. Il existe des méthodes bien moins élaborées et bien plus facile à mettre en oeuvre pour gagner de l'argent avec une attaque cyber. De plus en plus de recherches suggèrent que les cybercriminels se livrent à cette analyse coûts-avantages avant de se lancer dans une tentative nouvelle. Ainsi, il est peu probable que les organisations criminelles se lancent dans une entreprise de cette nature, étant donné que les récompenses sont (si) immatérielles [14] ;
- **Destruction -** La motivation probable d'une attaque de cette nature serait de causer de graves perturbations à l'état français. Étant donné le manque de motivation financière et les ressources nécessaires pour mener une perturbation de cette ampleur, il est fort probable que cette perturbation serait perpétrée par un gouvernement ou des groupes opérant sous le contrôle d'un état. Certains acteurs ont prouvé qu'ils étaient capable de telles attaques. De plus, ils pourraient quasiment opérer en toute impunité (remonter à la source dans une intrusion cyber est très compliqué) ;

52. voir partie 1.2, page 17.

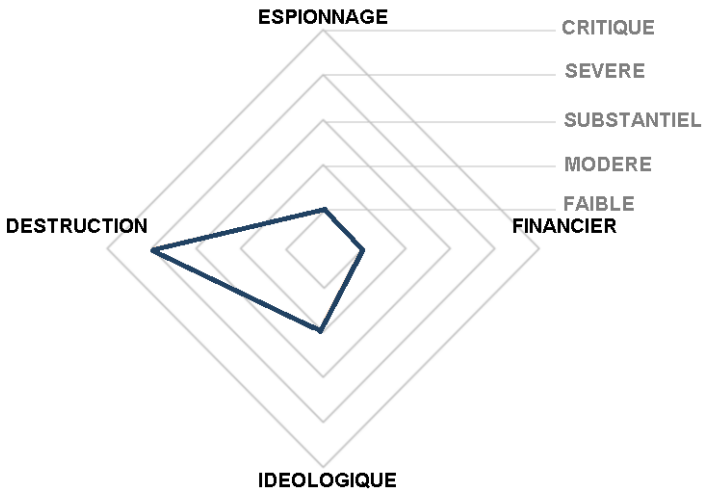


FIGURE 12 – Schéma des motivations pour l'attaque

Pour conclure, une attaque de cette ampleur nécessiterait une grande équipe (au moins plusieurs dizaines de personnes) qui travaillerait pendant plusieurs mois voire années à temps plein, avec de larges ressources et divers experts dans de nombreux domaines (l'expertise informatique, la langue française, la connaissance réseau, ...). Cela ressemble quasiment à un acte de guerre, sans vraiment de conséquence militaire en retour.

ENERGIE ET SERVICES PUBLICS

La perturbation cyber dirigée contre le réseau électrique ukrainien en 2015 [53] a confirmé un soupçon de longue date au sein du secteur de l'énergie selon lequel le réseau électrique pourrait être exposé aux attaques cyber d'agents sophistiqués.

Au sein même de la communauté internationale de l'énergie, il est reconnu depuis longtemps qu'une atteinte cyber de grande envergure est possible. En 2015, le Conseil mondial de l'énergie [54] a publié un rapport documentant les dangers potentiels pour les entreprises d'alimentation énergétique à l'échelle planétaire. Dans notre scénario, on estime que l'impact d'une intrusion cyber à large échelle serait proche de celui d'une destruction intentionnelle. A Paris en 2018, une violente coupure de courant a eu lieu à la gare Montparnasse suite à un incendie (destruction accidentelle). Les réparations ayant eu lieu sur plus de 3 jours afin de remettre le courant dans la gare, nous pouvons estimer qu'un incident cyber (destruction intentionnelle) de grande envergure durerait environ deux semaines avant d'être complètement maîtrisé.

53. "Un piratage informatique visant le réseau électrique ukrainien a provoqué une importante coupure d'électricité le 23 décembre dans la région d'Ivano-Frankivsk, dans l'ouest de l'Ukraine". Source : Le Figaro, Janvier 2016.
54. Source : World Energy Council, 2015.

Type d'attaque	Black-out
Motivation	Destruction
Région géographique	Île-de-France
Entreprise ciblée	EDF
Durée	15 jours

TABLE 10 – Résumé des caractéristiques choisies pour le scénario

Récupération de l'énergie, réparation du réseau

Lors de l'évaluation de l'ampleur des pertes économiques et des pertes d'assurance résultant de cette attaque, il faut principalement prendre en compte l'abilité des autorités françaises à fournir des sources d'énergie à court terme à la population et réparer ou remplacer les lignes de transport et de distribution endommagées. Ainsi, le processus de restauration, c'est-à-dire le temps nécessaire pour que la proportion de la population sans électricité revienne à des niveaux normaux (ici définis comme une couverture de 90% des ménages), est essentiel. En ce qui concerne la restauration de l'énergie et la réparation du réseau, nous allons décomposer ce travail en six points consécutifs pour tenter d'englober l'intégralité des spécificités du systèmes d'Île-de-France.

Afin de calculer une estimation de ce temps de restauration, nous allons utiliser un rapport mis en ligne par Lloyd's : *Emerging Risk Report : Business Black-out*, 2015. Cette étude analyse des évènements similaires ayant affecté les États-Unis depuis le début des années 2000. Nous allons analyser le profil de la courbe, les valeurs exactes n'étant pas adaptées au scénario français : le but étant donc de comparer les capacités des autorités françaises à réagir face à un tel évènement avec les résultats affichés par leurs homologues américains [24].

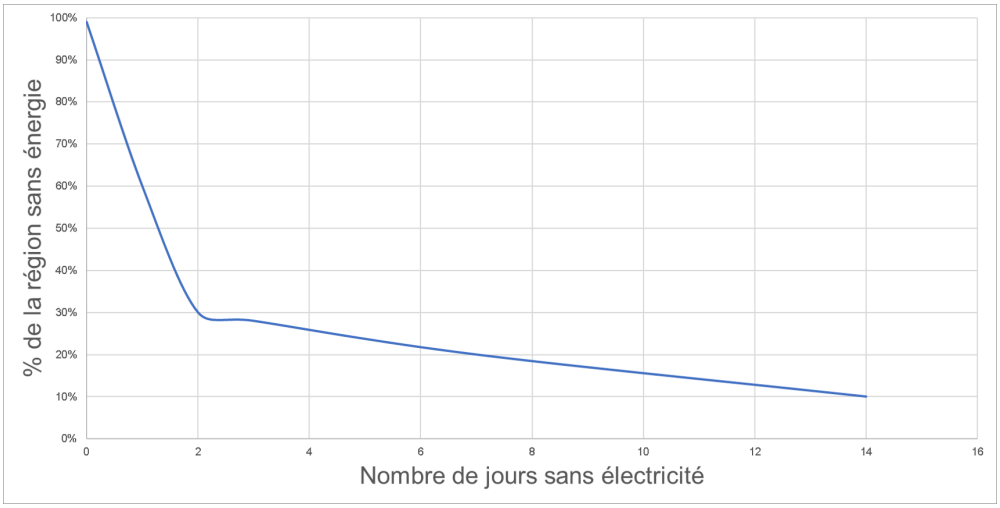


FIGURE 13 – Courbe des récupérations, durée d'une panne énergétique par scénario

Ainsi, plutôt que de prendre les courbes de restauration de panne d'électricité fournies par les

Lloyd's de Londres directement, nous allons les modifier pour créer un équivalent français pour l'Île-de-France.

Comparaison à l'international

Nous allons effectuer cette comparaison en deux temps : d'une part la comparaison du réseau français en terme de qualité de transmission de l'énergie, puis en nous intéressant à des indices de durée et de fréquence des pannes à Paris. Dans un premier lieu, nous pouvons affirmer que le réseau français n'est pas particulièrement robuste. On peut le voir notamment dans la figure ci-dessous [55] qui représente la qualité du transport de l'énergie, donc du réseau de distribution.

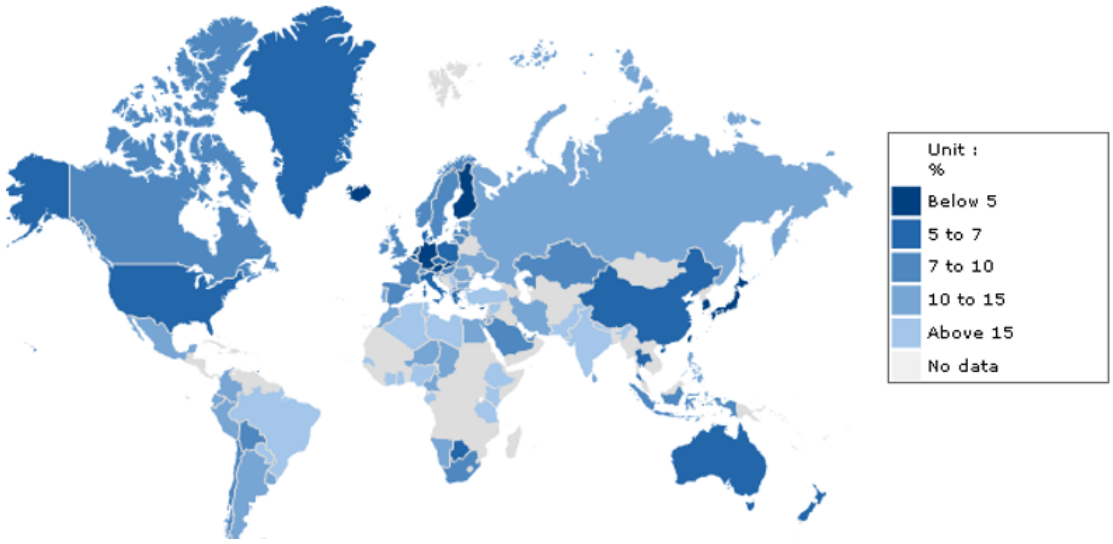


FIGURE 14 – Taux de pertes T&D d'électricité dans le monde

Le taux de pertes T&D d'électricité est le rapport entre la quantité d'énergie perdue pendant le transport et la distribution et la consommation d'électricité. On peut notamment comparer la France (7,6%) aux États-Unis (6,2%) pour faire le lien avec l'étude des Lloyd's et donc affirmer que la réaction de la France sera a priori moins performante.

En outre, malgré plus de pertes régulières sur le réseau de distribution, le système parisien est moins enclin à souffrir de pannes. Les indicateurs à prendre en compte sont l'indice de durée moyenne d'interruption du système (SAIDI [56]), qui examine la durée moyenne des interruptions par client servi, et l'indice de fréquence moyenne d'interruption du système (SAIFI [57]), qui le surveille du point de vue de la fréquence. Créés par l'Institut des ingénieurs électriciens et électroniciens (IEEE [58]), ces indices sont des outils précieux pour comparer la fiabilité des performances des utili-

55. Source : EnerData, 2015.
56. *System Average Interruption Duration Index.*
57. *System Average Interruption Frequency Index.*
58. *Institute of Electrical Electronics Engineers.*

taires électriques dans le monde entier. Ils se définissent de la façon suivante [59] :

$$SAIDI = \frac{Total\ duration\ of\ interruptions\ for\ a\ group\ of\ customers}{Number\ of\ all\ customers}$$

$$SAIFI = \frac{Total\ number\ of\ interruptions\ for\ a\ group\ of\ customers}{Number\ of\ all\ customers}$$

Pour la période 2012-2015 (la plus récente période de statistiques représentatives), la région de Paris surpasse celle de New York sur les deux indicateurs (voir le tableau ci-dessous [1]). En particulier, les bonnes statistiques de la région de Paris concernant la durée moyenne des pannes indiquent la capacité à réagir efficacement en cas de panne. Cela suggère que le réseau électrique français et la région de l'Île-de-France sont particulièrement bien placés pour faire face à une attaque de cette ampleur.

	Tokyo	New York	Paris	Londres	Berlin	Toronto
SAIDI	0,12	1,65	0,26	0,44	0,21	1,07
SAIFI	0,11	0,42	0,25	0,22	0,23	1,43

Table 11 – Comparaison des SAIFI et SAIDI des grandes métropoles entre 2012 et 2015

L'expérience Française

L'expérience française dans le domaine de gestion des catastrophes ou des crises est plutôt restreinte. En effet, du fait de leurs expériences en tant que victimes de catastrophes naturelles, les régions de New York ou de Tokyo par exemple sont mieux armées. L'unique véritable expérience de catastrophe naturelle est celle de Lothar en 1999, qui a affecté le réseau électrique et a failli plonger la capitale française dans un Black-out. Les équipes d'EDF limitent les dégâts, mais après l'interruption d'activité de trois centrales nucléaires et la coupure de réseau, 19 jours devront passer avant que tout ne soit réparé (contre 12 jours en moyenne aux États-Unis [9] pour des catastrophes naturelles similaires). La conséquence que nous pouvons en tirer est que la courbe équivalente pour l'Île-de-France devra avoir une silhouette plus allongée.

Le gouvernement français et les plans "Cyber Europe 2010" et "PIRANET"

L'intervention du gouvernement peut être un support de poids dans la gestion d'une crise énergétique comme celle présentée par notre scénario. En effet, cela fait parti de ses missions de protection de la population et du maintien de l'ordre public. En outre, le gouvernement français pourrait aider financièrement EDF à acquérir des fournitures essentielles telles que des pièces de rechange et des câbles T&D. Ceci est particulièrement important car les équipements de ce type sont généralement fabriqués sur mesure ce qui permet de suivre rapidement l'approvisionnement d'un

59. Source : *"SAIDI & SAIFI guiding towards more reliable distribution network"* Ensto, 2016.

grand nombre de machines des sous-stations, donc les câblages adaptés à l'infrastructure existante constitueront un défi à court terme pour EDF dans la gestion de la crise. Le gouvernement pourrait également aider à gérer la demande en imposant des restrictions sur l'utilisation de l'électricité afin de rétablir l'équilibre entre l'offre et la demande, ce qui pourrait réduire la panne d'électricité.

Le gouvernement a également organisé un "exercice de réponse à une crise majeure d'origine informatique" [60] en 2010. Selon le communiqué de presse, l'exercice consistait en une série de provocations afin de tester le plan "PIRANET" du gouvernement : plan d'organisation d'une réponse face à la cyber menace qui pèse sur la France. D'après le communiqué officiel, les réactions ont été satisfaisantes et les réponses adaptées.

D'autre part, l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) publie en 2010 un rapport sur le déroulement d'un "exercice de coopération européenne pour défendre nos réseaux" [61]. Ce scénario imaginé par l'ENISA [62] (*European Network and Information Security Agency*) présentait une attaque généralisée sur les points principaux de connexion entre les pays de l'Union Européenne. Le but étant de s'entraîner en cas de crise majeur et de savoir coordonner la réponse avec nos voisins dans un but d'efficacité et de pragmatisme. On pourrait également citer les exercices "Cyber Storm III" de 2010 dans les processus de préparation du gouvernement contre un risque informatique. Nous constatons ainsi que la France est dotée d'un système de réponse élaboré pour faire face à un sabotage de la sorte.

Les compteurs intelligents "Linky"

"Linky" est un compteur "intelligent" développé par Enedis qui pourrait s'avérer être un véritable atout dans la lutte contre le Black-out présenté dans ce scénario. En effet, en plus d'aider à la réduction de la consommation d'énergie, le grand nombre d'installation de ces dispositifs dans les foyers habités comme dans les entreprises [63] représente un grand nombre d'informations envoyées aux gestionnaires du réseau T&D ce qui permet un meilleur contrôle. Ce dispositif offre donc plusieurs possibilité comme le repérage plus rapide de la source, ou les informations de propagation de la panne par exemple.

Cela permettra également aux intervenants d'identifier les sources principales de demande qui créent un déséquilibre dans le réseau (et les désactiver le cas échéant), re-diriger le courant restant vers les installations clés telles que les hôpitaux et autres services d'urgence, et identifier les ressources disponibles.

60. Source : Secrétariat général de la Défense et de la Sécurité Nationale (SGDSN), Communiqué de presse, 2010.
61. Source : ANSSI, Communiqué de presse, 2010.
62. Agence européenne de sécurité de l'information et des réseaux.
63. Objectif d'équiper toute la France à l'horizon 2021.

Le processus de gestion d'incident

Alors que l'ampleur de l'évènement deviendrait immédiatement apparente au lendemain de l'attaque, les enquêteurs pourraient avoir besoin de temps pour identifier la source de l'échec. Pour ce faire, EDF devrait engager des enquêteurs spécialistes des sciences judiciaires pour déterminer l'origine de l'intrusion et s'assurer que toutes les "*backdoors*" sont fermées afin que les attaquants ne puissent pas revenir dans le système et provoquer à nouveau des coupures de courant. En conséquence, nous nous attendons à ce que le gouvernement établisse un équilibre entre la remise en marche du réseau énergétique et la nécessité d'éviter des incidents secondaires. Dans l'ensemble, nous pensons que cela retardera considérablement l'effort de rétablissement dans les 24 à 48 premières heures.

Courbe des récupérations

D'après les hypothèses évoquées et démontrées précédemment, nous nous attendons à avoir une courbe du même profil que celle des États-Unis présentée par les Lloyd's avec quelques différences :

- La France présente un réseau comportant plus de pertes régulières d'énergie que les États-Unis [64], donc moins performant face à une crise informatique ;
- L'Île-de-France (Paris) en revanche, a tendance à mieux gérer les situations de pannes, que ce soit en fréquence ou en durée, les interruptions du système électrique sont moindres [65] ;
- La France possède un faible historique de situation de crise comme le présente notre scénario. Elle n'est pas aussi habituée à faire face à de tels évènements que les États-Unis par exemple [66] ;
- Le gouvernement français a participé plusieurs fois à des exercices de préparation et de simulation de gestion de crise et prend cette menace très au sérieux. Cela indique que la France semble plutôt apte à se protéger et à répondre de manière cohérente à un scénario Blackout [67] ;
- Enfin, le développement de compteur communiquant [68] par Enedis aiderait EDF à gérer une perturbation de grande ampleur sur l'Île-de-France.
- Enfin, le fait que les études aient été menées il y a plusieurs années n'impacte pas sur notre approche. Nous estimons en effet que les méthodes de protection ont certes beaucoup progressé, mais la complexité et technicité des attaques également.

Nous résumons ces hypothèses dans le tableau ci-dessous.

64. voir figure 14 page 55.
65. voir tableau 11 page 56.
66. voir partie 5.2 page 56.
67. voir partie 5.2 page 56.
68. voir partie 5.2 page 57.

Facteur	Explication	Référence	Influence	Échelle
Qualité ordinaire	Transport d'électricité moins bon qu'aux US	Voir Figure 14 page 55	Translation horizontale	- 1
Situation de Panne	Meilleure gestion des pannes (SAIFI et SAIDI inférieurs)	Voir tableau 11 page 56	Translation verticale	+ 2
Historique	Île-de-France moins exposée aux catastrophes naturelles	Voir partie 5.2 page 56	Courbe moins pentue	- 3
Implication du gouvernement	Grande implication : exercices et programmes de défense réguliers	Voir partie 5.2 page 56	Translation verticale	+ 3
Particularité technique	Large présence de compteur intelligent	Voir partie 5.2 page 57	Courbe plus pentue	+ 2

TABLE 12 – Facteurs de modification de la courbe de restauration

Ainsi, nous estimons que la courbe des récupérations pour le scénario de Black-out sur l'Île-de-France devrait avoir le profil suivant :

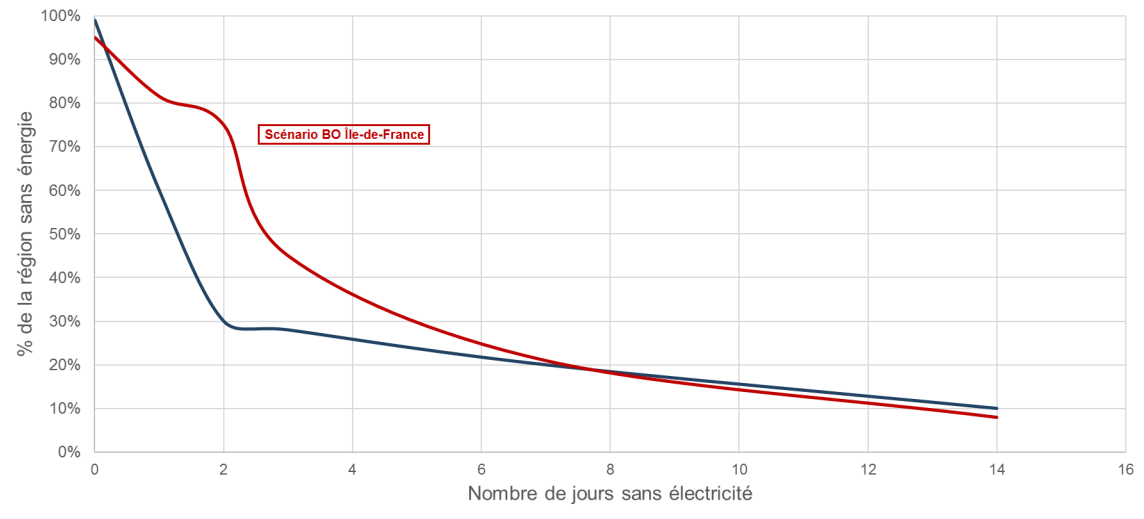


FIGURE 15 – Courbe des récupérations, scénario "BO Île-de-France", 2019

5.3 Pertes assurantielles

Suite à un évènement de cette ampleur, un grand nombre de demandes d'indemnisation seraient attendues sur diverses polices d'assurance. La sous-section suivante identifiera les secteurs d'activité touchés par l'attaque, puis clarifiera l'ampleur des pertes. Les particularités assurantielles des couvertures des victimes seront différentes de celles du document Black-out publié par Lloyds "Erebos" [24]. Ces pertes sont regroupés en quatre catégories de victimes :

(1)	Garantie dommage des entreprises	Les entreprises qui subissent des pertes à la suite du Black-out. Cela inclut la couverture des denrées périssables dans les restaurants et les supermarchés, les entreprises souffriraient a priori également de pertes d'activité.
(2)	Les entreprises indirectement affectées	Certaines entreprises en dehors de la zone accidentée mais touchées indirectement pourraient réclamer des dédommagements : par exemple si un fournisseur ou un client est atteint, cela peut causer de la perte d'exploitation.
(3)	Les propriétaires de polices MRH [69]	Les propriétaires de foyers pourrait réclamer des dommages et intérêts suite à la panne de courant. Par exemple sur l'électroménager, ou bien sur des dégâts matériels.
(4)	Polices spécifiques	Un certain nombre de couvertures spécifiques pourraient éventuellement être déclenchées à la suite d'un Black-out. Cela inclut la couverture "annulation d'évènements" par exemple. Nous pourrions également imaginer une augmentation des réclamations en RC Automobile (signalisation hors service), en assurance habitation (pillage, vol : les systèmes d'éclairage public et de vidéo surveillance ou d'alarme sont inutilisables), etc.. Mais nous estimons que ces pertes seraient négligeables.

TABLE 13 – Les différents types de demande d'indemnisation assurantielle

Travaillons à présent sur ces pertes assurantielles possibles. Nous allons nous concentrer sur la possibilité d'estimer, par catégorie, les réclamations probables des victimes.

(1) LES ENTREPRISES

Nous allons à présent voir comment ces pertes se traduisent dans la réalité de l'Île-de-France : Tout d'abord, la répartition des pertes ne serait pas uniforme dans tous les secteurs. Certaines industries résistent mieux aux coupures d'électricité que d'autres en fonction de caractéristiques clés.

	Agriculture	**Services**	**Finance**	**Industrie**
Part de la VA [70](Île-de-France)	0,20%	25,40%	18,90%	55,50%
Rendement pendant un BO	90%	60%	50%	40%

TABLE 14 – Capacité des grands secteurs d'activité à fonctionner pendant le Black-out [22]

Ainsi, la répartition est un élément essentiel influant sur la résilience de l'économie à un Black-out prolongée. Celle de la région Île-de-France est illustrée dans le tableau ci-dessus. Cela montre

69. Multi-Risque Habitation.
70. Part (%) de la Valeur Ajoutée, chiffres de l'INSEE, 2004.

que certains secteurs, tels que l'agriculture, peuvent fonctionner efficacement même en cas de panne d'électricité alors que d'autres secteurs tels que l'industriel sont fortement touchés.

En ce qui concerne les biens périssables (laboratoires, supermarchés, restaurateurs par exemple), le Black-out aurait un impact immédiat sur ces professionnels. Les biens perdus serait donc réclamés dans le cadre de l'assurance dommage. Les hypothèses de calculs sont détaillés dans la partie suivante avec l'application du scénario à un portefeuille.

Nous supposons que les polices PE qui comportent des exclusions cyber réussissent à ne pas répondre aux réclamations et n'entraînent aucune perte d'assurance. La couverture d'assurance du fournisseur suivrait la courbe de restauration décrite dans la section précédente (bien que des franchises soient appliquées) réduisant ainsi la gravité de la perte assurantielle.

(2) Les entreprises indirectement affectées

Les entreprises indirectement affectées pourront également poser des réclamations. Même si elles paraissent plus faibles, elles ne sont a priori pas négligeables. Les grandes installations ayant une assurance de biens avec une extension de PE peuvent également avoir une couverture "fournisseur critique". C'est une garantie distincte qui protège les entreprises qui perdent de l'activité en raison d'un non-respect des obligations de leurs fournisseurs principaux. Les fournisseurs clés en question doivent être nommés dans le cadre de cette police afin qu'elle se limite à un petit sous-ensemble de la chaîne d'approvisionnement du producteur. Bien sur, comme pour la couverture d'assurance précédente, si le cyber est exclu, nous nous attendrions à ce que cela soit maintenu. Les hypothèses seront également détaillées dans la partie suivante.

(3) Les propriétaires

La cause la plus probable des réclamations des propriétaires serait le résultat de la détérioration de la nourriture dans les réfrigérateurs et les congélateurs, mais également les dégâts sur les polices MRH. Les détails du calcul des pertes assurantielles en découlant sont présentées plus bas.

(4) Les polices spécifiques

De longues interruptions de service auront une influence sur les secteurs d'activité spécialisés, donc des polices spécifiques. Considérons qu'il s'agit principalement de la couverture d'annulation d'évènement : Les programmations faites en Île-de-France dans les jours suivant l'attaque risquent d'être annulés ou reportés à la suite de coupures de courant survenues dans la région. Le montant des répercussions de ce scénario fait l'objet d'un calcul démontré dans la prochaine partie.

Conclusion

Dans cette section nous avons donc présenté les étapes de calcul de la perte pour une perturbation hypothétique du réseau électrique de EDF dans la région de Paris. Le scénario présenté ici est extrême mais reste plausible et donne un aperçu des caractéristiques uniques du réseau électrique de l'Île-de-France.

Les hackers devraient mobiliser des ressources énormes, une stratégie adaptée et une compréhension approfondie du réseau de EDF et sa T&D pour mener une attaque de cette envergure. En conséquence, il est probable que cette atteinte soit l'œuvre d'acteurs étatiques visant à déstabiliser la France ou l'UE (on peut notamment penser aux JO de Paris 2024 par exemple). Une agression de cette ampleur serait extrêmement préjudiciable pour l'économie française, et ce pendant près de deux semaines. L'évènement entraînerait des sinistres d'assurance importants pour les catégories de dommages aux biens, de perte d'exploitation et plusieurs autres polices.

Bien que les pertes seraient probablement dévastatrices, certaines des caractéristiques uniques du réseau de EDF en Île-de-France et la planification du gouvernement français permettent de penser que les pertes seraient moins importantes qu'elles n'auraient pu l'être. Enfin, les relations conflictuelles (contrairement à un BO post-catastrophe naturelle) entre les pirates et les cibles (EDF et le gouvernement français) ajoutent une confusion supplémentaire post-attaque par la difficulté d'identifier la source, ce qui peut être critique au niveau économique et commercial mais également dans les relations diplomatiques internationales.

6 L'approche "fréquence $\times$ coût", modèle sur historique

Le modèle "fréquence $\times$ coût" basé sur l'historique est une méthode actuarielle permettant de déterminer une loi de distribution du nombre moyen de réclamations qu'un assureur recevra et en estimer une répartition probabilisée du coût moyen au cours d'un intervalle de temps, généralement un an. Un tel modèle prend en compte les spécificités du risque cyber en fonction du secteur d'activité, de la taille de l'entreprise mais aussi de sa localisation géographique.

6.1 Introduction à la construction du modèle

La seule branche du risque technologique pour laquelle nous pouvons espérer construire un modèle robuste est la perte de données (ou *"data breach"*, qui inclut également le vol). En effet, il s'agit de la seule menace cyber pour laquelle les actuaires possèdent quelques bases de données relativement complètes, et donc exploitables : depuis le début des années 2000, la notification dans le cas d'une intrusion cyber est obligatoire pour les entreprises américaines. Le recensement des incidents est donc effectué et nous pouvons travailler sur ces données. Ainsi, bien que les réglementations récentes en ce sens en Europe (RGPD en 2018) obligent à la notification des victimes, nous sommes pour l'instant contraints de concentrer notre travail sur le territoire américain.

Comme son nom l'indique, le modèle "fréquence $\times$ coût" se construit en deux temps : d'une part, nous allons travailler sur la partie de détermination de la fréquence d'occurrence des manipulations informatiques qui entraînent la perte de données : nous allons proposer une table de probabilités par secteur d'activité et taille d'entreprise. Ensuite, nous nous pencherons sur le coût de l'attaque afin d'obtenir une distribution de prix moyen par année par profil d'entreprise et l'appliquer à un portefeuille de polices cyber spécifiques.

Le cadre usuel d'utilisation des modèles "fréquence $\times$ coût" se présente de la manière suivante (avec S la sinistralité totale, N le nombre de risques, I_{C_i} l'indicatrice de survenance d'un sinistre grave et C_i le coût unitaire d'un sinistre grave) :

$$S = \sum_{i=1}^{N} I_{C_i} \times C_i \tag{1}$$

Ainsi, en fonction de i, nous avons $\mathbb{P}(I_{C_i} = 1)$ la probabilité de sinistralité sur le risque i (ici une ligne de notre portefeuille, donc une police souscrite) qui est le terme de "fréquence" et C_i le facteur de "coût".

Il est important de noter que faute de bases disponibles, nous allons nous appuyer sur des données américaines. Cependant, nous construirons des facteurs afin d'adapter ces hypothèses au marché français dans le but de faire tourner le modèle créé sur notre portefeuille client.

6.2 Détermination de la fréquence

Pour déterminer la fréquence d'une perte ou d'un vol de données aux États-Unis pour notre création de modèle "fréquence × coût", nous sommes partis d'une hypothèse législative : la notification de ces vols est obligatoire dans la plupart des états des États-Unis, et ce depuis maintenant de nombreuses années. Nous avons donc fait l'hypothèse que toutes les violations d'informations des entreprises américaines sur le territoire des États-Unis ont été déclarés et sont donc présents dans notre base de données. Ainsi, pour déterminer la fréquence des vols de données et donc la probabilité pour des professionnels d'avoir une réclamation auprès de leur assurance cyber, il suffit d'estimer la taille de l'échantillon concerné. Nous utilisons la loi de probabilité empirique suivante (pour l'exemple où A représente un incident cyber dans un secteur économique et pour une certaine taille d'entreprise) :

$$\mathbb{P}(A) = \frac{\text{Nombre de cas où A se réalise}}{\text{Nombre de cas possibles}} = \frac{Card(A)}{Card(\Omega)}$$

Mathématiquement, l'événement A est un sous-ensemble de Ω qui représente l'univers toutes les éventualités possibles. Donc ici, l'évènement A représente une perte de données dans une entreprise, et Ω le nombre d'entreprises entrant dans le cadre de l'étude.

(1) Le dénominateur

Ainsi, nous avons récupéré en source libre sur internet [71] une base de données nous permettant de connaître par secteur d'activité et taille d'entreprise, le nombre d'entités ayant leur siège social sur le territoire américain en 2016. Nous avons décidé de séparer les tailles d'entreprises en 4 catégories pour plus de précision. En effet, nous avons pu observer précédemment que le nombre d'employés influait sur son exposition à la violation de données. Nous avons donc regroupé nos entités selon les séparations internationales en fonction du nombre d'employés : Les TPE (Très petites entreprises, moins de 10 employés), les PME (Petites et moyennes entreprises, de 10 à 249 employés), les ETI (Entreprises de taille intermédiaire, de 250 à 4 999 employés) et enfin les GE (Grandes entreprises, plus de 5 000 employés) [72] ayant leur siège social aux États-Unis, en 2016.

	TPE	PME	ETI	GE
Nombre d'employés	< 10	10 à 249	250 à 4 999	> 5 000
Effectif	4 663 748	1 275 814	54 337	8 302
Effectif (%)	78%	21%	1%	0%

Table 15 – Définition et effectif des catégories de taille d'entreprise

71. *County Business Patterns*, 2016.
72. Ne pas confondre ces chiffres avec le nombre d'entreprise aux États-Unis, que Google estime à 28m.

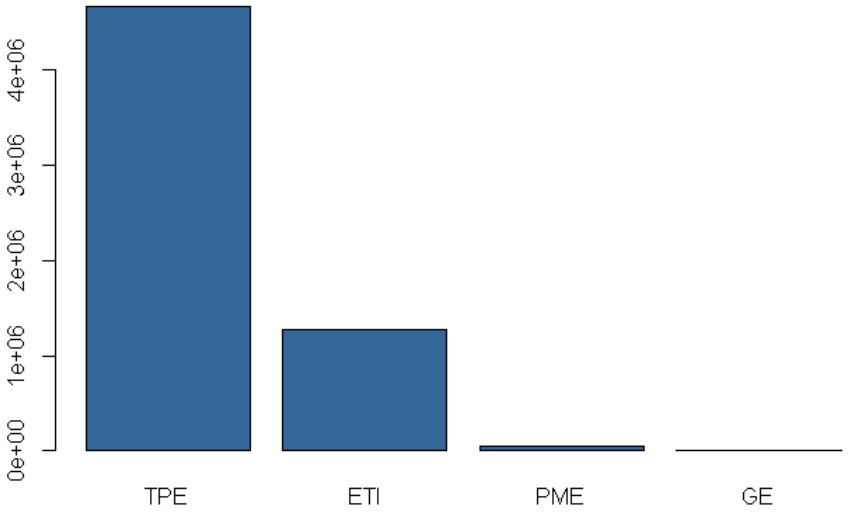


Figure 16 – Répartition des entreprises par taille aux États-Unis

Le secteur d'activité est identifié par le numéro NAICS [73]. Nous effectuons un travail de correspondance, et obtenons donc un total d'entreprises aux États-Unis en 2016, réparti en quatre groupes de taille d'entreprise et quatorze secteurs d'activité, qui sera le "tableau des dénominateurs" pour notre calcul de fréquence.

Fréquence - Dénominateur	
Base de données	County Business Patterns
Année	2016
Localisation	États-Unis
Hyp. Tailles d'entreprise	4 catégories
Hyp. Secteurs d'activité	13 domaines

Table 16 – Récapitulatif détermination de la fréquence - Dénominateur

(2) Le numérateur

Nous allons tout d'abord introduire les données qui nous ont servi de support pour paramétrer le numérateur dans ce modèle de fréquence.

Ce recueil d'information provient d'une base de données achetée par les équipes d'Aon travaillant sur le risque informatique, et remise en forme pour le bien de ce mémoire. Il s'agit d'un répertoire de 70 colonnes et 20 329 lignes répertoriant les incidents cyber reportés depuis le début des années 2000, dans le monde entier. Cette base, initialement conçue par RBS (*Risk Based Security*),

73. N*orth American Industry Classification System* : Le Système de classification des industries d'Amérique du Nord (SCIAN en français) est une nomenclature des activités économiques. Source : Wikipedia, 2019.

a été retravaillée par les équipes cyber de Aon *Analytics* aux Etats-Unis et en France [74]. A propos de la méthode de collecte de ces données, une technique automatisée de surveillance des sources qui diffusent ces informations permet d'actualiser la base de manière régulière et vérifiée.
Cette base de données comprend :

- des informations d'identification (Nom de l'entreprise, Secteur d'activité, ..) ;
- qualitatives (type d'attaque, type de perte, données atteintes, ...) ;
- quantitatives (Nombre d'employés, chiffre d'affaire, ...) ;
- temporelles (date de la première intrusion, date du report, ...) ;
- géographiques (adresse, région, pays de l'entreprise, ...).

Nous précisons que les filtres du pays (États-Unis) du type d'incident ("violation de données") ont été appliqués pour la construction de ce modèle, et la cohérence de nos hypothèses, ce qui n'empêche pas la base d'être suffisamment profonde pour que les études conservent tout leur sens.

Ci-dessous, un graphique en secteur représentant la contribution de différents pays sur le nombre d'incidents recensés dans notre base (avant le filtre). Nous pouvons remarquer immédiatement la large part occupée par les États-Unis. Cela rejoint ce que nous avons dit précédemment sur l'importance de ce sujet outre-atlantique, notamment sur la figure 3 de la page 25. Nous pouvons également noter le peu d'incidents cyber notifiés en France.

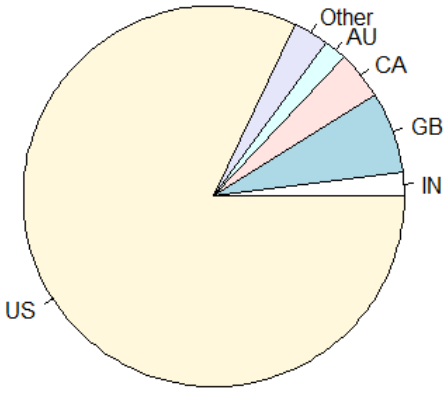


FIGURE 17 – Les principaux pays contributeurs de la base [75]

D'autre part, nous remarquons sur la figure ci-dessous que l'évolution du nombre d'incidents (reportés) de violation de données a largement évolué sur les dernières décennies, en croissant sans cesse. Nous pouvons imaginer que ce dernier va continuer à croître sur la même tendance exponentielle.

74. Nous ferons désormais référence à cette base en l'appelant "la base de Aon et RBS".
75. IN : Inde, GB : Grande Bretagne, CA : Canada, AU : Australie, US : Etats-Unis, *Other* : Autre (plus de 50 autres pays, dont la France).

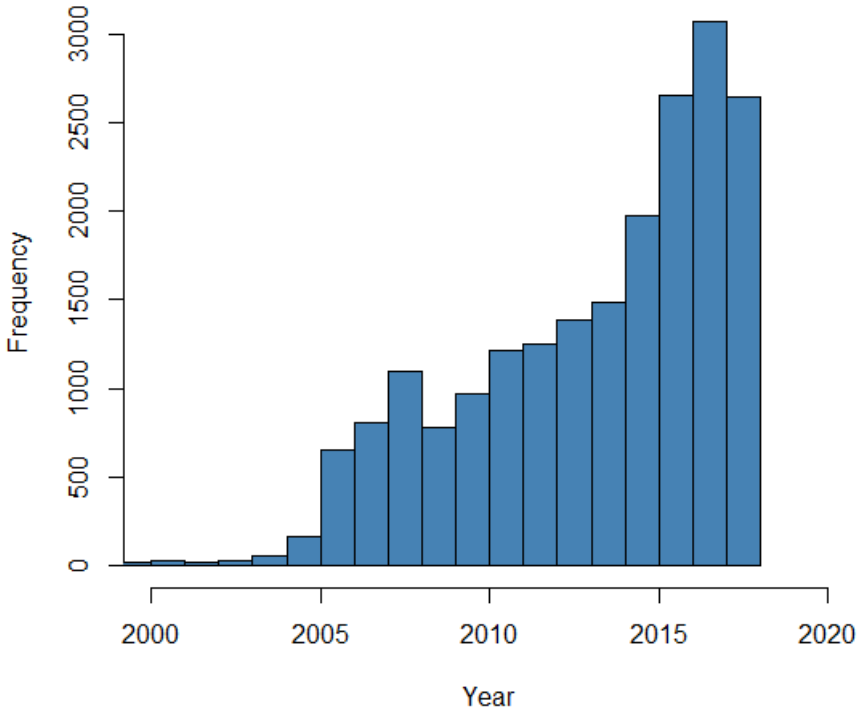


FIGURE 18 – Évolution annuelle du nombre d'incidents

Comme nous le voyons sur le graphique 18, le recensement de sinistralité est très pauvre. Il faut bien prendre en compte que ce n'est pas seulement qu'il y avait peu d'incident cyber, mais également le fait que leur notification n'était pas automatique ni réglementaire. La limitation en terme de données est en effet de l'un des grands challenges dans la modélisation de ce risque. Nous ne pourrons donc pas nous appuyer sur beaucoup d'historique et, au vu du graphique précédent, choisissons de conserver les quatre dernières années de pertes rapportées. Nous faisons également l'hypothèse que le nombre d'entreprises aux États-Unis n'a pas évolué de manière significative entre 2014 et 2017 et conserverons le tableau de dénominateur du nombre d'entités en 2016.

Enfin, nous possédons également l'information sur le secteur d'activité, et sur le nombre d'employés. Un travail de correspondance nous permet donc d'effectuer une répartition similaire à celle du dénominateur. Ainsi, la détermination de la fréquence sera possible par ces bases de données pour la construction de notre premier modèle.

Fréquence	
Base de données	Aon et RBS
Année	2019
Localisation	États-Unis
Historique conservé	2014-2017
Type de perte	Perte de données
Hyp. Tailles d'entreprise	4 catégories
Hyp. Secteurs d'activité	14 domaines

Table 17 – Récapitulatif détermination de la fréquence - Numérateur

Nous pouvons à présent dresser une première conclusion sur la construction de notre modèle : la première étape de détermination de la fréquence a été possible par l'exploitation de cette base de données américaine. Nous avons donc une probabilité d'occurrence d'un incident cyber de violation de données. Certes, quelques hypothèses (choix d'une telle base, séparation des secteurs d'activité de cette manière, distinction par taille d'entreprise, sélection des quatre années d'historique, nombre d'entreprise aux Etats-Unis constant entre 2014 et 2017 ...) ont été prises, mais les résultats obtenus présentés ci-dessous dans le tableau 18 semblent cohérents.

Pour conclure, voici le tableau récapitulatif du travail effectué sur la détermination de la probabilité d'occurrence d'un risque cyber :

Secteur d'activité \Taille	TPE	PME	ETI	GE
Agriculture & Exploitation minière	0,023%	1,408%	2,130%	0,004%
Services (Entreprise & Consommateur)	0,016%	0,085%	3,732%	11,861%
Éducation & Recherche	1,356%	1,373%	16,089%	21,505%
Finance	0,247%	3,749%	20,757%	31,954%
Santé	0,118%	0,344%	7,379%	65,497%
Industrie hôtelière	0,006%	0,130%	2,149%	4,375%
Industrie manufacturière	0,026%	0,101%	0,839%	2,211%
Associations à but non-lucratif	0,024%	0,042%	2,602%	5,469%
Édition	0,461%	2,051%	16,384%	14,869%
Commerce de détail	0,014%	0,231%	5,369%	19,777%
Services informatiques et logiciels	0,142%	0,062%	0,022%	0,026%
Transport	0,024%	0,506%	0,896%	1,278%
Utilité générale [76]	0,351%	1,209%	6,383%	3,175%
Commerce de gros	0,025%	0,057%	1,553%	4,530%

Table 18 – Tableau des fréquences d'occurrences annuelles d'incidents informatiques, par secteur d'activité et taille d'entreprise aux États-Unis

Les chiffres présentés ici sont les moyennes annuelles de fréquence d'incidents de violation de données en fonction du secteur d'activité et de la taille de l'entreprise : nous avons construit les fréquences pour les années 2014 à 2017 et en affichons ici les moyennes. Nous pouvons dès à présent observer les disparités en fonction de la taille (les grandes entreprises plus souvent ciblées) et du secteur d'activité (Finance, Santé plus souvent attaqués), facteurs discriminant dans l'exposition au risque cyber de violation de données. Ces remarques sont illustrées par la représentation graphique ci-dessous.

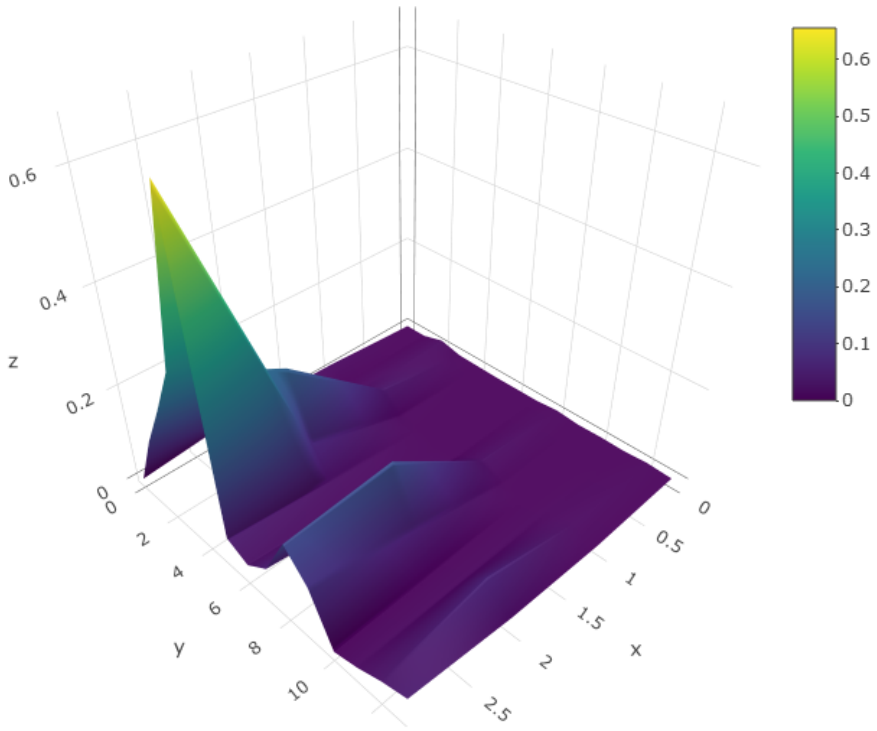


Table 19 – Représentation en 3 dimensions de la fréquence des vols de données (z) en fonction du secteur d'activité (y) et de la taille de l'entreprise (x), aux États-Unis

Dans notre modélisation, ces moyennes seront distribuées avec de la volatilité mesurée sur l'historique de sinistralité selon une distribution de probabilité (centrée sur la valeur affichée ci-dessus) : nous prenons l'hypothèse (forte) que la variabilité de la fréquence autour de cette moyenne ne dépend pas du secteur d'activité ni de la taille. Ainsi nous pouvons utiliser les fractions nombre d'incident reporté par nombre d'entreprise de tous les couples (Secteur d'activité ; Taille d'entreprise) sur les quatre années d'historique, et donc avoir suffisamment d'informations pour mesurer l'aléa et donc proposer une distribution sur les fréquences. Nous travaillons donc sur une unique série, après avoir normalisé les 224 observations (4 ans, 4 tailles d'entreprise, 14 secteurs d'activités).

Nous calculons le ratio de la variance sur l'espérance de ces observations afin de déterminer la

76. Ce tableau est une traduction des secteurs d'activité américain, mais en France, *Utilities* serait plutôt à interpréter comme les services publics.

loi discrète de fréquence la mieux adaptée à nos données selon la règle suivante :

$$R = \frac{\text{Variance}}{\text{Espérance}} = \frac{\mathbb{V}ar}{\mu} \tag{2}$$

- Si R < 0,8 : Nous utilisons une loi Binomiale ;
- Si 0,8 < R < 1,2 : Nous utilisons une loi de Poisson ;
- Si R > 1,2 : Nous utilisons une loi Binomiale Négative.

Pour mesurer la volatilité de nos observations et ainsi estimer une loi aléatoire adaptée, nous avons utiliser l'écart-type : ce dernier est dit homogène à la variable qu'il décrit, ce qui signifie que si toutes les observations sont multipliées par une même valeur $\alpha > 0$, l'écart type sera amplifié du même coefficient. Cependant, l'écart type est invariant par translation additive : si on ajoute une constante à toutes les observations, l'écart type demeure invarié. Ces deux propriétés en font un indicateur dit "de dispersion". Cet indicateur a donc été calculé dans le cadre de notre étude. Nous allons également devoir calculer le coefficient de variation, ainsi que la moyenne et la variance. Voici un résumé des différents indicateurs de cet ensemble de valeurs.

Moyenne (μ_{Tot})	4,26%
Variance ($\mathbb{V}ar$)	7,22%
Ecart-type (σ)	9,21%
Coef. de variation (c_v)	216,20%

TABLE 20 – Tableau récapitulatif des fréquences de *"data breach"*

Il est intéressant d'observer le coefficient de variation également nommé écart type relatif, qui est une mesure de dispersion relative, qui se calcule à partir de l'écart-type (méthode de Pearson) et de la moyenne (arithmétique) des observations l'échantillon :

$$c_v = \frac{\sigma}{\mu_{Tot}} = 2,16 = 216\%$$

Nous avons à présent le ratio qui nous intéresse :

$$\begin{aligned} R = \frac{\text{Variance}}{\text{Espérance}} &= \frac{\mathbb{V}ar}{\mu} \\ &= 169,48\% > 1,2 \end{aligned}$$

Ce dernier étant (largement) supérieur à 1, nous faisons donc l'hypothèse que la fréquence suit une loi Binomiale négative : la paramétrisation de cette distribution discrète de probabilité se fait avec deux facteurs. D'une part, l'entier naturel n non nul, et d'autre part un réel p tel que $0 < p < 1$. On peut également introduire $q = 1 - p$ la "probabilité complémentaire".

On note pour $k \in [0, n]$, lorsque $X \sim \mathbb{BIN}(n, p)$:

$$\begin{aligned} f_X(k; n, p) &= \binom{k+n-1}{k} p^n q^k \\ &= \frac{(k+n-1)!}{k!(n-1)!} p^n q^k \\ &= \binom{k+n-1}{n-1} p^n q^k \end{aligned}$$

Il est important pour le paramétrage, de noter que le lien entre les paramètres de la loi binomiale négative et son espérance et sa variance est le suivant :

$$\begin{aligned} \mathbb{E}sp = \mu &= \frac{r \times (1-p)}{p} \\ \mathbb{V}ar = \frac{\mu}{p} &= \frac{r \times (1-p)}{p^2} \end{aligned}$$

Nous allons donc générer par couple (Secteur d'activité ; Taille d'entreprise) une probabilité d'occurrence par une loi Binomiale Négative de paramètres $\mathbb{BIN}(r, p)$ tels que :

$$\begin{aligned} r &= \mu \times \frac{p}{1-p} \\ p &= \frac{\mu}{\mathbb{V}ar} = \frac{\mu}{(\mu_{Tot} \times c_v)^2} = \frac{\mu}{(\mu_{Tot} \times 216\%)^2} \end{aligned}$$

Ainsi, pour illustrer ce paramétrage de la loi de fréquence, prenons l'exemple suivant : Supposons l'entreprise A, une PME du secteur de la Santé. Sa probabilité moyenne d'être victime d'une violation cyber résultant en un vol de donnée est de $\mu = 0,344\%$. Ainsi, pour notre modèle, nous allons générer un tirage de la loi $\mathbb{BIN}(r, p)$, avec :

$$\begin{aligned} p &= \frac{\mu}{(\mu \times 216\%)^2} = \frac{0,344\%}{(4,26\% \times 216\%)^2} = 0,406 \\ r &= \mu \times \frac{p}{1-p} = 0,344\% \times \frac{0,406}{1-0,406} = 0,002 \end{aligned}$$

Nous avons ainsi une probabilité générée aléatoirement pour un incident cyber de violation de données par secteur d'activité et taille d'entreprise. Nous adapterons ces résultats à notre portefeuille dans la section d'application du modèle, notamment pour les rendre utilisables sur le marché français.

Une première conclusion sur la détermination de la fréquence

Nous pouvons remarquer plusieurs résultats après ce travail : dans un premier lieux, les plus hautes fréquences sont les secteurs d'activités les plus visés : il s'agit ici du *Retail Trade* (commerce de détail, sites de vente en ligne principalement), *Finance and Insurance* (données financières sensibles), et *Healthcare and Social Assistance* (données de santé sensibles). Cela semble cohérent avec

les articles d'actualité de presse spécialisée. En effet, ces domaines sont plus susceptibles de posséder des données intéressantes pour les voleurs : facilement revendable, et à un bon prix. A l'inverse nous pouvons relever les faibles nombres de tentatives de violation de données pour des secteurs comme l'art et le divertissement, ou l'agriculture, chasse et pêche. Enfin, nous constatons que les fréquences augmentent avec la taille de l'entreprise, ce qui semble cohérent vu que ces attaques ciblent les détenteurs de grosses bases de données dans le but de les voler puis les revendre ou les bloquer puis en demander une rançon. Nous observons graphiquement ces remarques dans le *heatmap* ci-dessous. Nous voyons également la grande volatilité des fréquences d'incidents cyber en fonction du secteur d'activité et de la taille de l'entreprise.

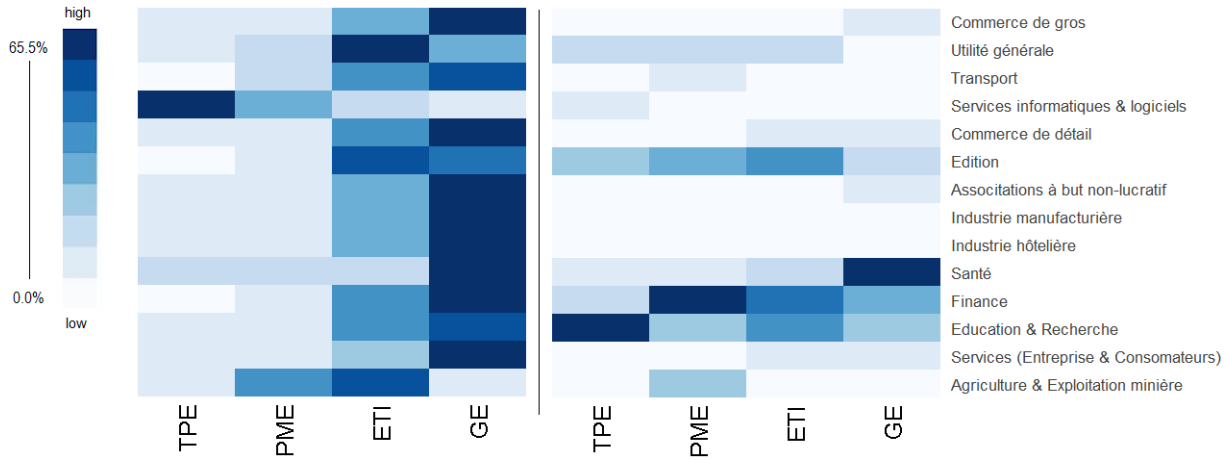


TABLE 21 – *Heatmaps* des fréquences d'occurrences annuelles d'incidents informatiques, par secteur d'activité (droite) et taille d'entreprise (gauche) aux États-Unis

Pour conclure, nous avons déterminé une loi aléatoire pour générer la fréquence d'occurrence d'un incident cyber de violation de données pour toutes les entreprises, classées par secteur d'activité et nombre d'employés. Nous avons fait cela à partir de bases de données relativement récentes et profondes. La distribution déterminée est paramétrée sur les entreprises américaines, pour la violation de données. Nous pouvons à présent passer à la détermination des facteurs de coût pour estimer les montants de pertes potentielles.

6.3 Détermination du coût

Il faut tout d'abord comprendre que dans le cas des *data breaches* (ou "violation de données"), le coût de la perte se décompose en deux parties : il y a d'une part la quantité d'information volée (c'est-à-dire le nombre d'enregistrements dérobés), mais également la sensibilité (le coût de la donnée perdue) de cette dernière. En effet, certaines informations sont plus sensibles que d'autres et donc coûtent plus chères, donc sont en général mieux protégées. Ainsi, comme nous l'avons vu dans la

formule 1 (page 63), le montant S du sinistre se définit de la manière suivante :

$$S = \sum_{i=1}^{N} I_{C_i} \times C_i$$

Formule que nous adaptons en prenant en compte avec la décomposition du coût en la multiplication de la quantité d'information volée par le coût unitaire de la donnée volée :

$$\begin{aligned} S &= \sum_{i=1}^{N} I_{C_i} \times C_i \\ &= \sum_{i=1}^{N} I_{C_i} \times T_i \times c_i \end{aligned}$$

6.3.1 Détermination de la taille de la base de données compromise

Le graphique ci-dessous est extrait de la base de données de Aon et RBS, on s'intéresse à la variable **Total_Affected**, qui traduit la taille de la base dérobée. Cette variable étant d'amplitude très grande (gros volume de chiffre) et toujours positive, nous avons choisi d'en étudier le logarithme, pour en quelques sortes la lisser et la rendre plus facile à étudier.

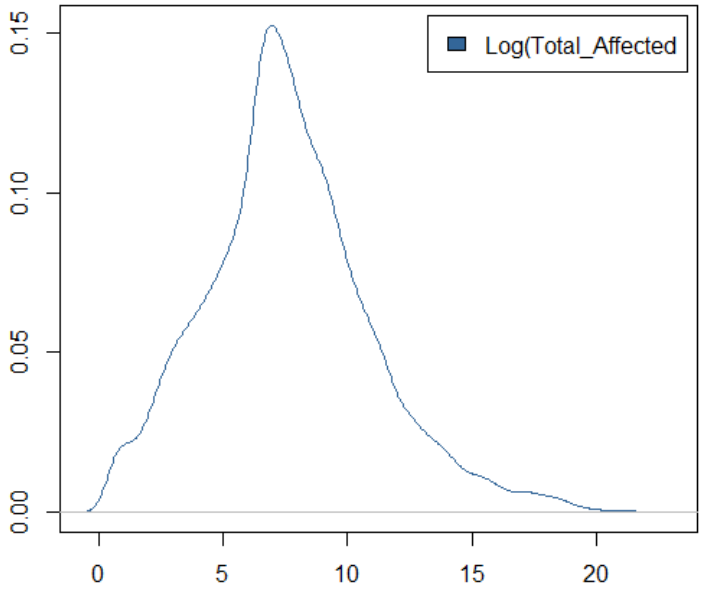


FIGURE 19 – Densité de probabilité de la taille de l'échantillon volé

Nous allons ajuster une loi de probabilité pour cette courbe de densité, en cherchant le modèle le plus adapté. Après avoir essayé tout un panel de lois de probabilité, certaines sont automatiquement écartées après observation des graphiques d'ajustement (Weibull, Beta, ...). Cependant, d'autres lois usuelles semblent plus adéquates (meilleure dispersion notamment) et feront donc l'objet de tests statistiques pour déterminer la plus adaptée. Ainsi, pour notre étude, nous avons choisi de tester

les trois distributions suivantes : les lois Normale, Gamma et Logistique.

La loi Normale $X \sim \mathcal{N}(\mu, \sigma^2)$.

La loi Normale est une loi de probabilité absolument continue qui dépend de deux paramètres : $\mu \in \mathbb{R}$ son espérance, et son écart-type $\sigma \in \mathbb{R}^+$. Sa densité de probabilité est données par la formule suivante :

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} \exp^{-\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2} \tag{3}$$

La loi Gamma $X \sim \Gamma(k, \theta)$.

La loi Gamma (ou plutôt la famille des distributions Gamma) est caractérisée par deux facteurs : le facteur de forme $k \in \mathbb{R}^+$, et le facteur d'échelle $\theta \in \mathbb{R}^+$. Sa fonction de densité est la suivante (avec Γ représentant la fonction Gamma d'Euler) :

$$\forall x > 0, f_{k,\theta}(x) = \frac{x^{k-1} \exp^{-\frac{x}{\theta}}}{\Gamma(k)\theta^k} \tag{4}$$

La loi Logistique

La loi Logistique est une distribution absolument continue à support infini. Elle possède deux paramètres d'emplacement (la moyenne μ) et d'échelle (un réel $s > 0$)[77]. Sa fonction densité est exprimée ainsi :

$$f_{\mu,s} = \frac{\exp^{-\frac{x-\mu}{s}}}{s\left(1 + \exp^{-\frac{x-\mu}{s}}\right)^2} \tag{5}$$

Nous affichons ci-dessous, sur l'histogramme de la distribution des logarithmes des tailles de violations, les trois courbes de nos lois pour un premier jugement visuel de l'adéquation.

77. La loi de distribution logistique ne possède pas de paramètre de forme ; en conséquence, la fonction de densité ne prend qu'une forme : cette dernière est semblable à celle de la loi Normale. Cependant, la loi de distribution logistique présente des extrémités plus longues.

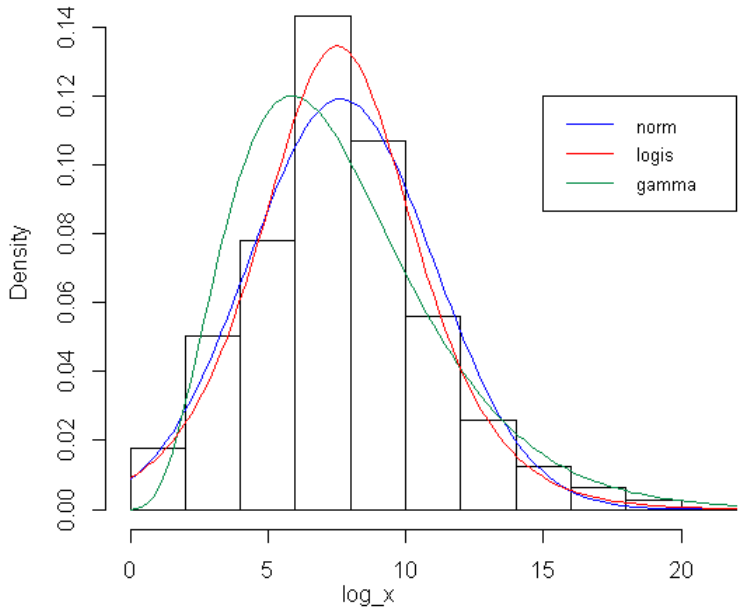


FIGURE 20 – Superposition des courbes estimées sur le logarithme du nombre d'enregistrements volés

Nous pouvons remarquer en premier lieu qu'aucune des trois lois ne peut immédiatement être écartée après la comparaison à la distribution empirique de notre base de données. En statistique, l'estimateur du maximum de vraisemblance permet de trouver les valeurs des paramètres d'une loi de probabilité qui maximisent la fonction de vraisemblance avec l'échantillon empirique de données. La fonction de vraisemblance est définie de la manière suivante : Soit $C = \{c_1, ..., c_k\}$ un ensemble fini, $\{P_\theta\}$ une famille de lois de probabilité sur C, et n un entier. On appelle vraisemblance associée à la famille $\{P_\theta\}$, la fonction qui à un n-uplet $(x_1, x_2, ..., x - n)$ d'éléments de C et à une valeur θ associe la quantité :

$$L(x_1, ..., x_n, \theta) = \prod_{i=1}^{n} P_\theta(x_i)$$

Le premier graphique permet d'observer graphiquement l'adéquation de la courbe paramétrée (en rouge) et l'échantillon empirique de données sous forme d'histogramme. Sur le *Q-Q plot* (quantiles théoriques par rapport aux quantiles empiriques) nous voyons que les points se positionnent sur la première diagonale, donc la distribution théorique choisie est pertinente. De même pour le *P-P plot* (fonction de répartition théorique par rapport à la fonction de répartition empirique) : bon alignement sur la première médiatrice tout écart indique une différence entre les distributions.

A présent, afin de juger l'adéquation entre la loi paramétrée et l'échantillon empirique, nous allons procéder à un test statistique. Le test de Kolmogorov-Smirnov permet cela en utilisant la fonction de répartition continue. Nous déterminons une hypothèses 0 dites "hypothèse nulle", on la note H_0.

Hypothèse H_0 : Les deux échantillons que nous testons proviennent de la même loi : les distributions empiriques et théoriques sont les mêmes.

Ensuite, nous recherchons des preuves que cette hypothèse devrait être rejetée ou non et nous l'exprimons en terme de probabilité. Si la probabilité que les échantillons proviennent de distributions différentes dépasse un certain niveau de confiance, nous demandons que l'hypothèse initiale soit rejetée en faveur de son opposée H_1 qui présente les deux échantillons comme deux extraits de distributions différentes.

Ce test s'appuie sur les propriétés des fonctions de répartitions empiriques. Soit $X_1, ..., X_n$, n variables indépendantes identiquement distribuées définies sur un espace de probabilité $(\Omega, \mathcal{A}, \mathbb{P})$, à valeurs dans $\mathbb{R}$, avec F_X pour loi de répartition. La fonction de distribution empirique F_n de $X_1, ..., X_n$ est telle que :

$$\forall x \in \mathbb{R}, \forall \omega \in \Omega, F_n(x, \omega) = \frac{\text{nb éléments} \leq x \text{ dans l'échantillon}}{n} = \frac{1}{n} \sum_{i=1}^{n} \mathbb{1}_{X_i(\omega) \leq x} \tag{6}$$

Notons $F_n(x, .)$ la variable aléatoire $\omega \to F_n(x, \omega)$. On obtient la convergence (également vraie pour max au lieu de sup) de :

$$\lim_{n \to \infty} \mathbb{P}\left[sup_x |F_n(x, .) - F(x)| > \frac{c}{\sqrt{n}} \right] = \alpha(c) = 2 \sum_{r=1}^{+\infty} (-1)^{r-1} \exp(-2c^2 r^2) \, \forall c \in \mathbb{R}^+ \tag{7}$$

Ci-dessous les résultats de nos tests statistiques pour voir l'adéquation des lois construites sur nos données empiriques de tailles des violations. Le p-Value p est la probabilité (sous H_0), d'obtenir une statistique aussi extrême que la valeur de l'échantillon (on peut aussi l'interpréter comme le plus petit seuil de significativité pour lequel l'hypothèse nulle H_0 est approuvée). On choisit un seuil de significativité α, puis on compare p et α :

- $p < \alpha$, on ne peut pas accepter l'hypothèse, donc on rejette H_0 ;
- $p > \alpha$, on approuve H_0

Nous choisissons un seuil d'acceptation (ou "de significativité") $\alpha = 5\%$ pour notre étude.

	Normal	**Gamma**	**Logis.**
D	0,048128	0,090513	0,027629
p-Value	0,0179	0,0226	0,1979

TABLE 22 – Résultat du test de Kolmogorov-Smirnov

Le risque de rejeter H_0 alors que l'hypothèse est vérifiée est dit "de première espèce". Si dans notre cas toutes les lois semblaient graphiquement satisfaisantes, nous voyons à présent au seuil

d'acceptation (fixé à 5%) que seule la loi Logistique est acceptable :

$$\text{p-Value}_{Logis} = 19,8\% > 5\%$$

Nous allons donc la privilégier pour la création de notre modèle. Voici ci-dessous ses paramètres.

	Estimation	**Erreur standard**
Paramètre 1	7,53224	0,03203663
Paramètre 2	1,858506	0,01549501
AIC : 52,89		
BIC : 62,91		

TABLE 23 – Paramètres de l'ajustement de la loi Logistique estimée par maximum de vraisemblance

Pour une étude plus approfondie de l'adéquation nous avons également étudié d'autres courbes nous permettant de mieux comprendre le comportement des lois.

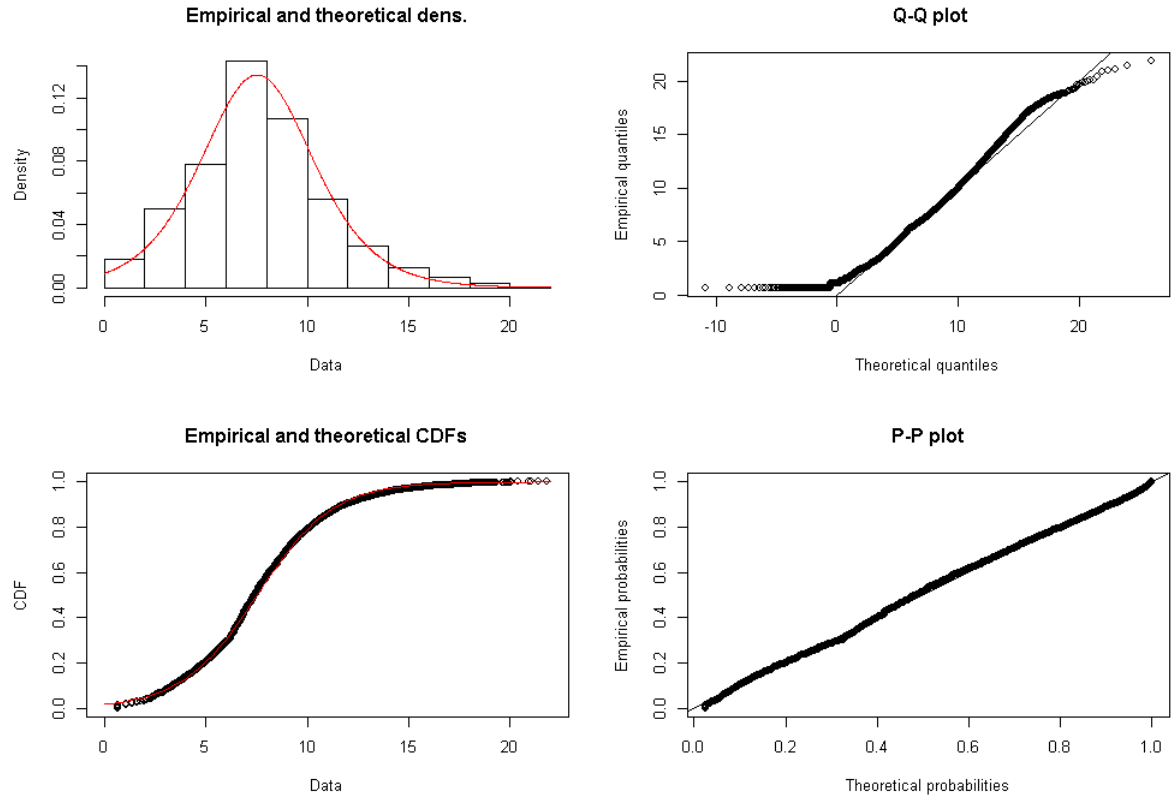


FIGURE 21 – Résumé de l'adéquation de la distribution **Logistique**

Ce résumé de l'adéquation de la distribution Logistique nous permet d'observer la qualité de

l'ajustement effectué par la méthode du maximum de vraisemblance [78].

Tout d'abord, notons bien que la transformation de la loi Logistique en la loi log-Logistique se fait en changeant le paramétrage de la manière suivante :

$$X \sim \text{logis}(\mu, s) \Rightarrow e^X \sim \text{log-logis}\Big(\alpha = e^{\mu}, \beta = \frac{1}{s}\Big),$$

Ainsi afin d'obtenir une estimation de l'ampleur de la perte, nous pourrons donc générer une loi log-Logistique avec les paramètres α (*location*) et β (*scale*) suivant :

Paramètres	**Valeurs**
Distribution	log-Logistique
Location (α)	$\alpha = e^{7,53}$
Scale (β)	$\beta = \dfrac{1}{1,86} = 0,54$

TABLE 24 – Les paramètres de la distribution log-Logistique pour l'estimation du nombre d'enregistrements volés

Nous pouvons relever également l'information sur les critères AIC, BIC et de log-vraisemblance : leur valeur intrinsèque n'est d'aucun intérêt puisqu'ils ne sont calculés qu'à des fins comparatives. En effet, le critère d'information d'Akaike mesure la qualité d'un modèle statistique. Plus le critère AIC est faible, plus le paramétrage est jugé adapté. Il se calcule théoriquement avec la formule suivante :

$$\text{AIC} = 2k - 2\ln L$$

Avec k le nombre de paramètres à estimer du modèle et L le maximum de sa fonction de vraisemblance. D'autre part, nous avons le BIC (Critère d'information bayésien), qui propose une pénalité en fonction de la taille de l'échantillon utilisé (ce que ne prend pas en compte le critère AIC). Il se présente comme cela :

$$\text{BIC} = -2\ln L + k \times \ln N$$

Avec L la vraisemblance du modèle estimée, N le cardinal de l'échantillon et k toujours le nombre de paramètres libres du modèle. De même, le modèle qui minimise le critère bayésien sera préféré.

78. A des fins de comparaison, nous avons également étudié ces résultats pour les autres adéquations. Une annexe est à disposition en fin de rapport, et contient les autres résumés d'adéquation des distributions. Voir annexe N : "Adéquation des lois".

	AIC	**BIC**
Normal	53,18	64,11
Gamma	59,10	69,26
Logis.	52,89	62,91

TABLE 25 – Comparaison des critères d'erreurs

Nous avons bien dans nos résultats $\text{AIC}_{logis} < \text{AIC}_{norm} < \text{AIC}_{gamma}$ et $\text{BIC}_{logis} < \text{BIC}_{norm} < \text{BIC}_{gamma}$. Cela confirme notre choix de la loi log-Logistique.

Coût - Taille de l'échantillon volé	
Base de données	Aon et RBS
Année	2019
Localisation	États-Unis
Hyp. Tailles d'entreprise	4 catégories
Hyp. Secteurs d'activité	14 domaines
Hyp. Loi aléatoire	Loi Log-Logistique

TABLE 26 – Récapitulatif détermination de la taille de l'échantillon volé

Ainsi, après avoir étudié la quantité d'information perdue (la taille de la violation), nous allons nous concentrer sur le coût unitaire de ces données.

6.3.2 Détermination du coût unitaire moyen par profil d'entreprise

L'étude *"Ponemon Institute Releases 2019 Cost of Data Breach : Global Analysis"* [20] révèle en 2019 que le coût de chaque enregistrement perdu ou volé contenant des informations sensibles et confidentielles, est en moyenne de 163 USD en France (soit environ 146 EUR). Le coût total d'une violation de données a augmenté de 8,39% en France sur les dernières années (depuis 2017) [79], pour atteindre une moyenne de 3,85 m EUR sur l'année civile. Ponemon étant l'institut de référence sur le marché, nous utiliserons cette observation moyenne comme base de détermination du coût. Nous appliquerons un facteur d'aggravation sur ce prix moyen, en fonction du secteur d'activité et de la taille de l'entreprise [80].

Avant cela, nous pouvons constater la relation entre la taille de l'échantillon volé et le montant moyen individuel de la donnée. En effet, le graphique ci-dessous illustre le nombre de données dérobées lors d'attaque cyber par le score de sévérité de la perte. Le score de sévérité représente la

79. IBM Security et Ponemon Institute *"Cost of Data Breach Report"*, 2019.

80. Notons également que nous n'aurons donc pas besoin d'appliquer un facteur d'adaptation au paramètre du coût moyen pour l'application au portefeuille client dans la partie suivante, ce dernier étant déjà issu d'une étude spécifique au marché français.

sensibilité de la donnée dérobée (et donc traduit son coût), il est mesuré par les équipes de RBS à partir du type d'information perdue. Les données utilisées pour effectuer le graphique ci-dessous sont issues de la base d'Aon et RBS. Nous y remarquons une nette corrélation entre la taille de l'échantillon et la gravité pécuniaire de l'intrusion [81].

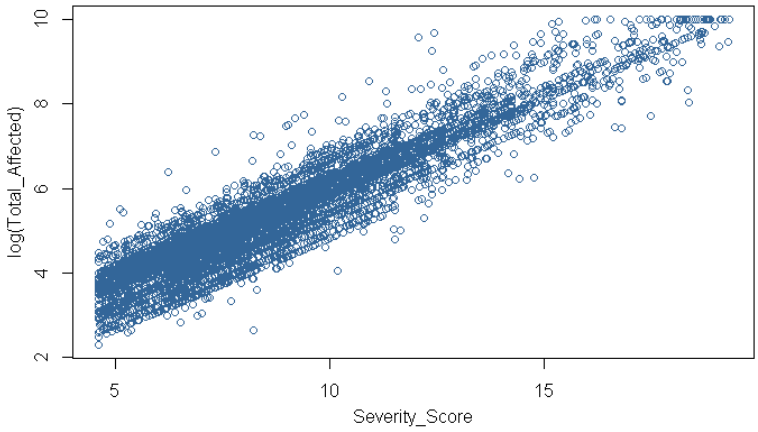


FIGURE 22 – Nombre d'enregistrements en fonction du *Severity_Score*

Le manque de données effectuant le lien entre le coût total du vol et le nombre d'enregistrements nous empêche de construire une véritable relation quantifiable entre les deux grandeurs. En revanche, le *boxplot* ci-dessous nous permet de réaliser que les gros vols en terme de nombre d'enregistrements concernent plutôt des données peu sensibles, et inversement. Ce graphique provient de l'open data "Information is beautiful" [82] sur le risque cyber au cours de la dernière décennie (recensement depuis 2011). Il s'agit d'une base de données de 6 105 enregistrements et 11 colonnes. Ce regroupement est composé d'informations concernant uniquement les vols de données aux US. La sensibilité de la données dont nous nous servons ici est représentative de son coût : en effet, les violations concernant des données de sensibilité élevée sont des informations plus précieuses, plus rares et donc plus chères. Le tableau ci-dessous résume la composition des différentes catégories, desquelles nous pourrions en déduire un impact sur le coût moyen.

Sensibilité	Composition
1	Adresses mails, numéro de sécurité social, identifiants pour sites gratuits et publics...
2 / 3	Informations bancaires incomplètes, Compte Paypal/Ebay, informations de sites marchands, numéros de téléphones, dates de naissance ...
4 / 5	Informations bancaires complètes, données de santé, ...

TABLE 27 – Catégories et composition de la variable de sensibilité

81. Coefficient que nous ne pouvons pas calculer puisque nous ne possédons pas de base de données liant à la fois le coût du *data breach* (total ou unitaire par enregistrement) et le nombre de données volées.

82. Site en ligne offrant des bases de données en libre accès, notamment sur le sujet du cyber. Base téléchargée en 2019.

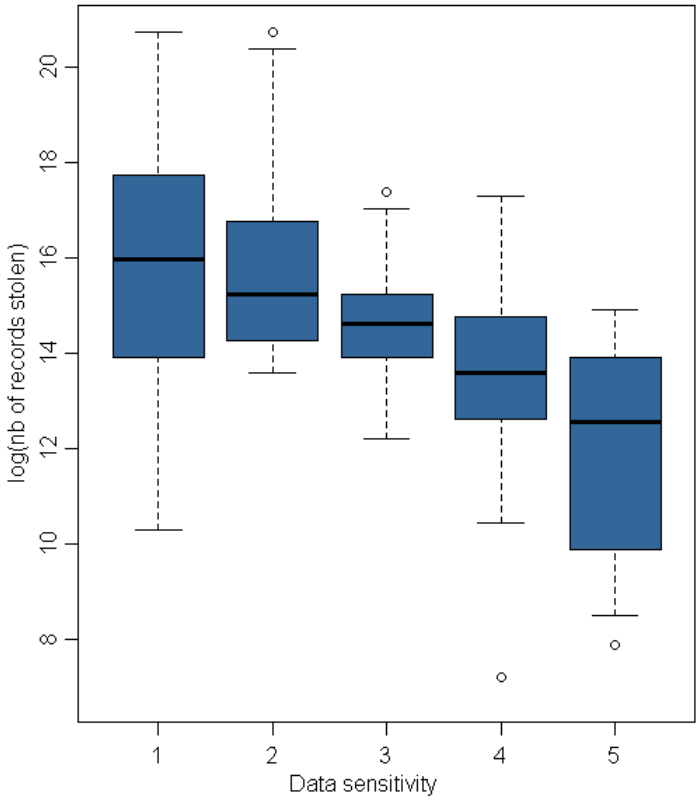


FIGURE 23 – *Boxplot* de la taille de l'échantillon en fonction de la sensibilité des données volées

Ainsi nous concluons que nous ne pouvons pas construire une véritable corrélation mathématique entre le montant individuel d'une donnée dérobée et la taille de l'échantillon, mais nous devons tout de même prendre en compte cette relation. Nous allons donc construire des paliers de coût moyen, en fonction du nombre d'enregistrements compromis. Ainsi, les violations touchant moins de 798 000 enregistrements (premier quartile) seront considérées d'un montant moyen de 25% plus cher que les 146 EUR moyens. De même les violations de plus de 13 670 000 enregistrements (troisième quartile) seront pris en compte à 25% moins cher que la moyenne générée. Ainsi, nous conservons le montant moyen publié par *Ponemon Institute* pris en hypothèse précédemment, tout en prenant en compte cette corrélation.

Min.	1er Qu.	Médiane	Moyenne	3e Qu.	Max.
934	798 000	3 000 000	40 433 000	13 670 000	1 000 000 000

TABLE 28 – Récapitulatif des tailles des bases volées

Nous pouvons remarquer dans le tableau ci-dessus que la moyenne est particulièrement élevée. Nous soulignons qu'elle excède le troisième quartile (largement). La moyenne n'est donc pas représentative, mais plutôt la médiane pour comprendre la taille d'une violation de données.

Taille de la base victime	Coût moyen par enregistrement
< 798 000	110 EUR
798 000 < .. < 13 670 000	146 EUR
> 13 670 000	182 EUR

TABLE 29 – Résumé des coûts unitaires de la donnée en fonction de la taille de la base

Nous avons donc réussi à obtenir une loi permettant de générer aléatoirement un nombre d'enregistrements volés par attaque cyber. Nous avons également fixé (en prenant certaines hypothèses) un coût moyen par enregistrement en fonction de l'importance de la base de données dérobées. Intéressons-nous à présent aux variations de ce coût moyen en fonction du secteur d'activité et de la taille de l'entreprise victime.

Création du facteur d'aggravation de coût

La base de Aon et RBS nous permet de présenter ci-dessous une matrice représentant un coefficient de coût de perte de données par secteur d'activité et taille d'entreprise. En effet, dans cette base de données, un indicateur (intitulé "$Severity\_Score$" dans la base) représente l'importance pécuniaire de la perte : il est construit par les créateurs de la base décrit ainsi : "les infractions sont notées sur une échelle de 1 à 10, indiquant la gravité relative de l'incident.". Indépendant du nombre de données volé, il traduit directement la sensibilité de la données atteinte. Nous pouvons donc construire un facteur de sévérité (d'aggravation) qui inclura la variabilité du coût d'une donnée perdue en fonction du secteur d'activité et de la taille de l'entreprise victime. En normalisant cet indicateur autour de l'unité , nous le transformons en facteur que nous pouvons multiplier au coût moyen d'une donnée dérobée en France nous obtenons une granularité par domaine d'activité et nombre d'employés.

Secteur d'activité \Taille	TPE	PME	ETI	GE
Agriculture & Exploitation minière	0,86	0,91	1,03	0,99
Éducation & Recherche	0,94	1,00	0,91	0,88
Finance	0,97	1,12	1,02	1,03
Santé	1,06	1,01	1,03	1,00
Industrie hôtelière	0,96	0,87	1,09	1,05
Industrie manufacturière	0,96	0,98	1,37	1,22
Associations à but non-lucratif	1,04	1,09	1,02	0,99
Édition	1,10	1,09	1,02	1,09
Commerce de détail	1,01	1,03	0,97	0,94
Services informatiques et logiciels	1,08	1,06	1,04	1,07
Transport	1,13	1,19	1,12	1,11
Utilité générale	0,96	1,03	1,24	1,00
Commerce de gros	0,95	0,89	0,95	0,97

TABLE 30 – Table du facteur de sévérité du coût de l'incident, en fonction du secteur d'activité et de la taille de l'entreprise

Le *heatmap* ci-dessous offre une représentation graphique du tableau de résultat des facteurs de sévérité moyens observés sur l'échantillon empirique. Elle permet d'afficher les disparités entre les différents couples (Secteur d'activité ; Taille d'entreprise). La volatilité de ces données est faible mais nous avons adapté notre coefficient de nuance de couleur afin d'observer les écarts existants.

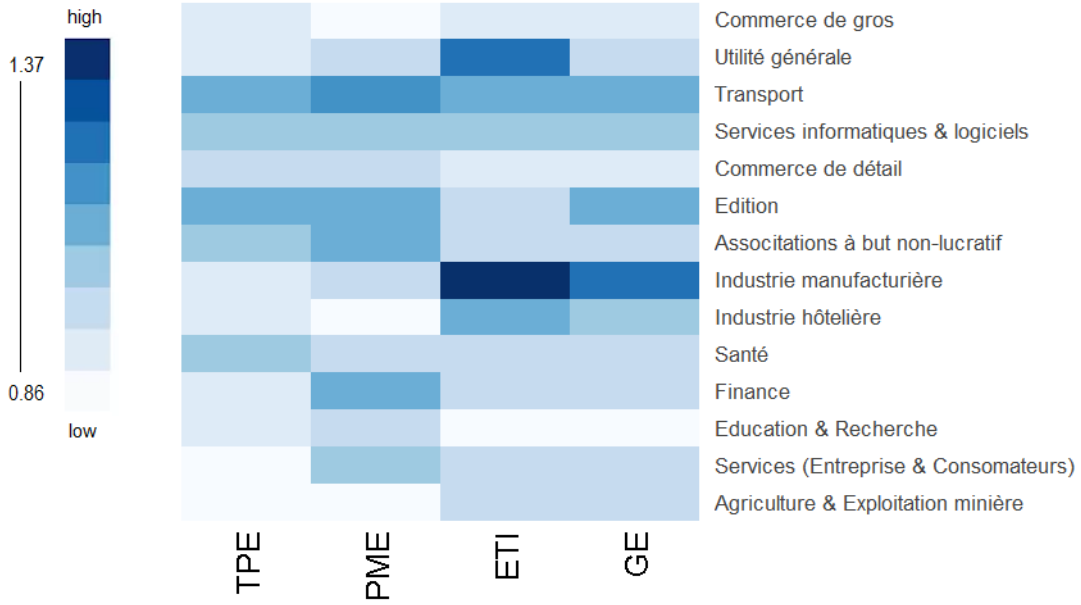


FIGURE 24 – *Heatmap* du facteur de sévérité du coût de l'incident, en fonction du secteur d'activité et de la taille de l'entreprise

De même que pour l'estimation de la probabilité d'occurrence, nous avons affiché dans le tableau récapitulatif ci-dessus des valeurs moyennes pour les facteurs de sévérité. Nous allons y introduire de la volatilité par la même méthode que précédemment, en calculant le coefficient de variation sur l'historique après normalisation. Nous l'utiliseront ensuite pour déterminer la variance de la loi centrée en chaque valeur du tableau pour générer les facteurs de sévérité de nos sinistres dans la modélisation : nous avons cette fois-ci besoin d'une loi continue, donc nous n'utiliserons pas la même règle mais allons paramétrer une loi Normale qui semble la plus adaptée à notre situation. Nous vérifierons tout de même que la loi paramétrée remplit les critères d'adéquation.

Ci-dessous l'adéquation de la distribution Normale sur nos données. Nous pouvons remarquer sur le diagramme Q-Q (Quantile - Quantile) que les points sont alignés sur la première bissectrice (ce qui signifierait que la distribution suit probablement une loi gaussienne normalisée), ce qui soutient l'hypothèse de la loi Normale. D'autre part, si on se penche sur l'analyse du graphique P-P, on peut évaluer l'asymétrie de notre distribution comme quasiment nulle. En effet, ce diagramme est une fonction de probabilité qui évalue la concordance de deux ensembles d'informations en traçant leurs fonctions de distribution cumulative : l'hypothèse par rapport à l'échantillon observé. A nouveau, même si le résultat n'est pas absolument parfait, il n'est pas révélateur d'un empêchement majeur pour nous ou d'une incohérence dans l'utilisation de la distribution Normale.

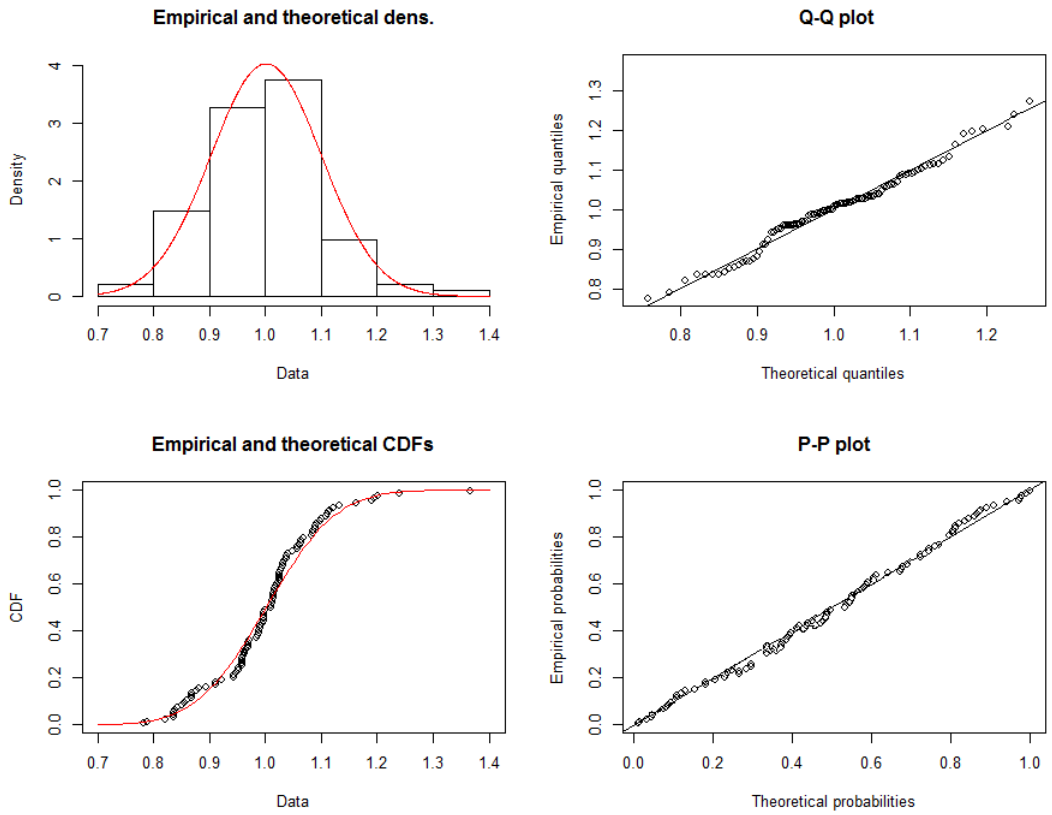


FIGURE 25 – Résumé de l'adéquation de la distribution Normale pour le facteur d'adaptation du coût moyen

Ci-dessous, les paramètres d'ajustement de notre loi sur la distribution empirique. Nous pouvons voir qu'avec la méthode de maximum de vraisemblance, les erreurs d'estimation sont très faibles. L'analyse des *P-Plot* et *Q-Q plot* ainsi que l'étude de différents indicateurs nous permet donc de confirmer que l'hypothèse de la loi Normale n'est pas aberrante.

	Estimation	Erreur standard
Espérance	1,00000	0,009836
Variance	0,098854	0,006952

TABLE 31 – Paramètres de l'ajustement de la loi Normale estimée par maximum de vraisemblance

Nous allons donc utiliser une loi Normale pour estimer la variabilité et générer aléatoirement le facteur d'amplification du coût de l'incident. Ses paramètres seront déterminer de la sorte : nous concentrerons l'espérance sur le tableau 30 (moyenne du facteur de sévérité par taille d'entreprise et secteur d'activité) et nous laisserons la variance comme nous l'avons déterminée dans le paramétrage ci-dessus, c'est-à-dire d'environ 10%. Nous pouvons remarquer plusieurs résultats de ce tableau 30, mais la lecture point par point n'est pas forcément très pertinente à commenter. Nous noterons surtout que la volatilité est assez importante dans ces valeurs, et que donc les coûts sont

variables dans les violations de données, en fonction de l'entreprise victime.

Le *heatmap* (figure 24) représente graphiquement cette volatilité et la disparité observable entre les différents couple (Taille d'entreprise ; Secteur d'activité). Nous allons donc appliquer un coefficient (généré aléatoirement) pour les secteurs d'activité où les informations sont plus chères (comme par exemple la santé) ou bien pour les entreprises où la taille joue un rôle dans le montant payé [83]. Nous pouvons souligner certains secteurs qui semblent plus coûteux (Santé, Finance, Banque) que d'autre (Immobilier, Construction, Agriculture). De plus, nous pouvons également remarquer les disparités au niveau des tailles d'entreprises : en effet, dans certains secteurs, les TPE vont être plus fortement touchées, quand les GE le seront plus dans d'autres. Nous pouvons remarquer qu'en moyenne générale (pondérée) les incidents sur ETI sont plus coûteux que sur les GE. On explique cela notamment par les meilleurs moyens de défense, et déclenchement de cellules de gestion de crise plus efficaces.

Coût - Facteur de sévérité	
Base de données	Aon et RBS
Année	2019
Localisation	États-Unis
Hyp. Tailles d'entreprise	4 catégories
Hyp. Secteurs d'activité	13 domaines
Hyp. Loi aléatoire	Loi Normale

Table 32 – Récapitulatif détermination du coût - Facteur de sévérité

Quelques conclusions intermédiaires

Nous conclurons de manière générale sur la construction et l'emploi de cette modélisation à la fin de ce chapitre. Entre temps, nous pouvons tout de même énoncer quelques remarques. Nous avons à présent les paramètres du modèle, et ainsi une modélisation fonctionnelle que nous allons appliquer à un portefeuille de garanties spécifiques cyber afin d'estimer le coût de ces couvertures, et le risque de cumul porté. En revanche, nous pouvons émettre plusieurs réserves en ce qui concerne le travail effectué dans cette sous-partie. D'une part, le coût moyen publié par *IBM Security* et l'institut *Ponemon* est issu d'études statistiques sur le marché. Nous ne savons rien de plus que ce qui est dit dans l'étude et donc ne pouvons pas garantir ce chiffre. D'autre part, la base de données étant limitée en profondeur, tous les secteurs d'activité ne sont pas bien représentés et les sorties sont donc imprécises. Enfin, nous avons retrouvé à plusieurs reprises les barrières du manque de données qui nous ont poussé à prendre plusieurs hypothèses.

83. Attention, il ne s'agit pas de doubler le travail effectué sur la probabilité d'occurrence d'un incident informatique mais bien sur le coût moyen d'une intrusion. En effet, l'impact de la taille et du secteur d'activité de l'entreprise sur la probabilité d'une attaque est prise compte dans la partie de calcul de la fréquence de l'intrusion.

Troisième partie

Application au portefeuille : adaptation au marché français, présentation des résultats et analyse comparative

7 Application du scénario à un portefeuille de marché

Nous allons à présent estimer l'impact de notre scénario sur les engagements. Le but étant de quantifier l'exposition d'une telle population, pour ultérieurement fixer les limites de garantie en réassurance en fonction de l'appétence au risque de la compagnie. L'application du scénario permet également de mesurer l'empreinte, les pertes maximales probables et le risque de cumul sur l'ensemble du portefeuille.

7.1 Application et résultats

Dans cette partie, on soumet le portefeuille présenté au filtre des pertes assurantielles décrit dans le scénario "BO Île-de-France". Nous allons implémenter le modèle afin de voir ces calculs par type de demande d'indemnisation :

(1) Les entreprises

D'une part, les entreprises directement affectées par le Black-out. Au ligne à ligne nous avons effectué le processus suivant pour la garantie perte d'exploitation :

1. Pour les entreprises concernées (Île-de-France) on prend le chiffre d'affaire annuel [84] (CA_{annuel}) que l'on rapporte à un CA journalier ($CA_{journ.}$) :

$$CA_{journ.} = \frac{\text{Chiffre d'affaire Annuel}}{\text{Nombre de jours dans l'année}} = \frac{\text{CA}_{annuel}}{365}$$

2. Calcul de la perte journalière pendant le Black-out par entreprise : on multiplie le CA journalier par l'opposé complémentaire de l'efficacité de chaque secteur (voir tableau 14) : soit i un secteur d'activité, et r_i son rendement pendant le BO.

$$\forall i, \forall r, PE_{journ.} = CA_{journ.} \times (1 - r_i)$$

3. On calcule les pertes par jour au fil des réparations, avec la courbe de restauration (voir courbe

84. Il est évident que si nous possédions une information plus précise (chiffre d'affaire mensuel ou journalier par exemple) nous l'utiliserions. En effet, les CA ne sont pas toujours distribués uniformément sur une année.

15) : en considérant R_k le taux de restauration le k-ième jour sans électricité depuis le début du Black-out (N = 14, le nombre de jour que dure le BO),

$$\forall i, \forall r, PE_{BO} = \sum_{k=1}^{N} PE_{journ.} \times r_i \times (1 - R_k)$$

4. On résume les pertes quotidiennes par entreprise et on applique les conditions de la police d'assurance (franchise et limite). On note F_j et L_j respectivement la limite et la franchise du contrat d'assurance cyber pour la PE de l'entreprise j, et on obtient donc le versement de garantie suivant pour la police concernée :

$$\forall j, G_{PE_j} = \min(\max(PE_{BO} - F_j; 0); L_j)$$

5. Pour mesurer le risque porté par le portefeuille (J = 50 000, nombre d'entreprises) au titre de garantie cyber pour la PE, nous sommons l'ensemble de ces sinistres, pour obtenir le montant total des réclamations (S_{tot} : sinistre total) :

$$S_{tot} = \sum_{j}^{J} G_{PE_j}$$

Pour ce portefeuille de 50 000 lignes, à partir des hypothèses présentées précédemment, nous obtenons des réclamations cumulées totales d'un montant de

$$S_{tot} = 44\ 012\ 394 \text{ EUR}$$

A titre indicatif, il peut être à présent intéressant de se pencher sur le montant de la prime d'assurance individuelle moyenne (P) pour une telle couverture dans ce portefeuille : une police cyber *"Stand Alone"* (spécifique) pour la perte d'exploitation :

$$\text{P} = \frac{\text{Montant total des réclamations}}{\text{Nombre de polices concernées}} = \frac{S_{tot}}{J} = \frac{44\ 012\ 394}{50\ 000} = 880{,}25 \text{ EUR}$$

Il convient de réaliser maintenant que même si cette prime est calculée avec des hypothèses fortes et de manière simplifiée, cette prime pure demeure particulièrement élevée pour le marché français. De plus, nous n'avons ici pas pris en compte les marges commerciales et autres majoration, mais nous sommes intéressés seulement au prix technique. En effet, les couvertures cyber PE s'échangent pour seulement quelques dizaines d'euros. Bien sur, la prime commerciale propre (finale) dépend de la taille de l'entreprise (son chiffre d'affaire) et de son secteur d'activité, de son

secteur géographique, et surtout du marché.

D'autre part, le secteur d'activité le plus touché pour **la garantie de dommages aux biens** serait les établissements mal protégées par le différentiel de tension (en majorité les restaurants et les magasins de la grande distribution -agro-alimentaire-). Admettons que ce sont les seules entreprises qui souffriraient du BO pour cette couverture. Nous travaillerons en partant de l'hypothèse que la grande majorité de ces firmes ont une assurance "dommages" et que 95% [85] de ces entités ont des générateurs d'énergie indépendants qui continueront à fonctionner pendant un certain temps et donc pourront protéger l'alimentaire.

Un groupe électrogène moyen alimenté au diesel tient environ 14 jours au carburant et serait en mesure de couvrir le temps d'arrêt prévu décrit dans notre scénario. Nous nous attendons également à ce qu'une partie des générateurs ne fonctionne pas correctement après l'attaque. Au moins 15% des établissements dotés d'installations de production d'énergie souffriraient de panne. Nous supposerions également que la demande de nouveaux générateurs et de pièces de rechange serait excessive, ce qui rend les réparations ponctuelles extrêmement difficiles. On peut donc considérer le nombre d'installations sinistrées ($N_{inst.}$) soit (i un compteur des établissements d'agro-alimentaire de la région Île-de-France) toutes les entreprises qui ont un groupe électrogène (Ent_i) indépendant fonctionnel (Gen_i) , soit :

$$\begin{aligned} N_{inst.} = \text{Card}\Big(\bigcup_i Ent_i \cap Gen_i\Big) &= \sum_i \text{Card}\Big(Ent_i \cap Gen_i\Big) \\ &= \sum_i \mathbb{1}_{Ent_i} \times \mathbb{1}_{Gen_i} \end{aligned}$$

Ce qui signifie que la proportion de commerces touchés (toutes les sociétés sauf celles qui ont un générateur d'énergie indépendant et fonctionnel) est le suivant :

$$P = 1 - 95\% \times (1 - 15\%) = 19,25\% \approx 20\%$$

Ainsi, nous considérons que la part de toutes les installations qui souffriraient potentiellement d'un contenu détérioré s'élèvent à 20%. Ce montant serait alors extrêmement difficile à estimer, puisqu'il s'agit de stock perdu.

Dans notre portefeuille nous n'avons pas d'entreprise d'agro-alimentaire donc le problème ne se pose pas. Nous estimons donc d'après les hypothèses présentées dans le paragraphe précédent que la garantie dommages aux biens ne joue que de façon trop négligeable dans le scénario "BO Île-de-France" sur ce portefeuille en particulier.

85. Source : étude *"TEPCO Black-out Scenario"*, Stroz Friedberg Ltd Aon, 2018.

Enfin, pour les professionnels, nous pouvons également prendre en compte la **responsabilité civile professionnelle** (RCP) : il s'agit d'une garantie présente dans le portefeuille choisi pour l'illustration. La RCP couvre tout préjudice causé à autrui dans le cadre de l'activité de l'entreprise. Si en effet on ne peut pas blâmer les entreprises d'être responsable du BO, on peut leur reprocher de ne pas avoir su mettre en place une protection adaptée avec les moyens nécessaires pour protéger leurs clients, ou leurs employés : on peut imaginer dans une usine par exemple un ouvrier travaillant avec des robots. Le Black-out peut entraîner des dommages corporels car la sécurité du robot est défaillante. Les pertes ici sont extrêmement négligeables puisque le chemin est long et difficile pour prouver la responsabilité de l'établissement. Nous estimons donc que les réclamations en RCP sont nulles pour notre portefeuille.

(2) Les entreprises indirectement affectées

Dans la catégories des garanties pour les sinistres des entreprises indirectement affectées, nous nous concentrons principalement sur la **couverture "fournisseur critique"**. Nous n'avons pas cette police en portefeuille, l'exposition est donc nulle et donc pas de charges d'assurance pour notre portefeuille en raison d'entreprises indirectement affectées. Notons tout de même que de telles garanties pourraient faire l'objet de perte.

(3) Les propriétaires

Il semblerait que la **garantie "perte des denrées dans un congélateur"** de l'assurance habitation soit la seule couverture impactée dans notre scénario pour les propriétaires. En effet, toute panne dépassant 24 heures pourrait endommager le contenu du congélateur. La période au-delà de ce point est en grande partie sans conséquence sur l'ampleur de la perte car tous les dommages sont causés au cours de cet intervalle initial (1,5 jour disons). Pour identifier les pertes de ce scénario, supposons que le niveau des dommages subis par le ménage suive exactement la courbe de restauration. En conséquence, on prendra les 75%[86] plus gros comptes de propriétaires. En supposant qu'une partie seulement des ménages concernés déposent une réclamation, nous estimons qu'environ 50% demandent un remboursement au titre de leur police MRH. Par conséquent, on sélectionnera le plus grand des $75\% \times 50\% = 32,5\%$ comptes et supposera que les propriétaires réclament la limite maximale. Il s'agit d'un portefeuille de professionnels, il n'y a donc pas de particulier dans ce schéma. Donc pas de réclamation à ce titre dans notre illustration.

(4) Les polices spécifiques

Nous supposerions que tout évènement comportant une assurance annulation d'évènement dans la zone de Paris au cours des 12 jours suivant l'incident serait reporté dans ces circonstances. Comme le scénario est aléatoire quant à la date d'occurrence, nous supposerions que 3% de toutes les polices seraient touchées ($12/365 = 3\%$ jours). Par conséquent, nous considérons les 3% les plus impor-

86. Lecture sur la courbe des réparations (figure 13), après 1,5 jours.

tants de ces évènements (sur la base de la rémunération totale en cas d'annulation) et supposons la perte totale. Dans ce portefeuille, il n'est pas question de cette garantie, nous n'avons donc pas de perte dans cette catégorie.

7.2 Conclusions sur le modèle par scénario

Pour conclure sur cette première approche, nous pouvons tout d'abord présenter la sinistralité escomptée moyenne pour une attaque Black-out : 44 012 394 EUR. Il s'agit comme présenté précédemment des pertes assurantielles estimées. Notons que la forme de la courbe de restauration présentée dans ce chapitre souligne la différence entre le type de dégâts causés par une attaque cyber comparée par exemple à une catastrophe naturelle. Ces coûts sont principalement dûs aux garanties de pertes d'exploitation et de gestion de crise. En effet, comme nous l'avons mentionné au cours de ce chapitre, les entreprises perdraient a priori plusieurs heures (qui pourraient même se compter en jours) d'activité et donc de revenus. L'impact d'un tel scénario semble donc vraiment conséquent et permet de soulever la problématique de l'importance des assurances cyber [87].

D'autre part, nous avons évoqué précédemment la difficulté de remonter à la source d'une attaque cyber. Le problème se pose ici lorsque les compagnies d'assurances vont se tourner vers le fautif de ces différents sinistres. Nous pouvons penser que certains assuré se plaindront vers EDF pour demander des comptes quant à cette coupure inopinée. Ainsi, il est intéressant d'imaginer la démarche de l'assureur d'EDF qui sera contraint à indemniser ces victimes, sans pour autant que le coupable puisse un jour être démasqué.

Enfin, la conclusion d'une approche par scénario peut être effectuée en trois points principaux : nous nous servons de ce type de modèle de sinistralité pour révéler l'exposition silencieuse et estimer les pertes maximales probables. Ce type d'approche est très utilisé sur le marché de la réassurance. Un scénario permet notamment à la réassurance de fixer les plafonds de garanties, puis la priorité (et à aider les compagnies d'assurance à fixer les franchises) en fonction de l'appétence de l'agent sous-jacent et de son aversion au risque. Le second point est une comparaison marché des limites trouvées, et in fine le dernier une comparaison avec l'historique des pertes connues. L'approche par scénario a l'intérêt de dévoiler les expositions silencieuses, mesurer l'exposition au risque de cumul, et donc de permettre de mieux se couvrir pour une entreprise ou une compagnie d'assurance.

87. Notons tout de même que l'impact du Black-out ne se limite pas aux pertes présentées dans ce rapport, de nombreux autres réclamations seraient faites aux compagnies d'assurance. Voir Annexe O : "Scénario : pertes assurables additionnelles".

Sensibilité de la sinistralité aux hypothèses

Pour conclure, avant de présenter l'application des autres approches, il convient de rappeler que ces résultats sont issus d'une modélisation contenant plusieurs hypothèses assez importantes. Il est intéressant d'étudier la sensibilité de ces résultats aux hypothèses.

Pour cela, nous avons repris les différents paramétrages du scénario "*Black-out Île-de-France*" et nous proposons une vision plus sévère (scénario "*up*") puis plus optimiste (scénario "*down*"). Notons que les hypothèses "*up*" et "*down*" sont également pertinentes. Voyons d'une part l'influence sur la courbe de restauration :

		Échelle		
Facteur	**Influence**	Standard	"*up*"	"*down*"
Qualité ordinaire	Translation horizontale	- 1	- 1	0
Situation de Panne	Translation verticale	+ 2	+ 1	+3
Historique	Pente courbe	- 3	- 4	-2
Implication du gouvernement	Translation verticale	+ 3	+1	+3
Particularité technique	Pente courbe	+ 2	+ 1	0

TABLE 33 – Facteurs de modification de la courbe de restauration

Cette modification des facteurs se traduit graphiquement par le déplacement de la courbe et la déformation de la pente de cette dernière.

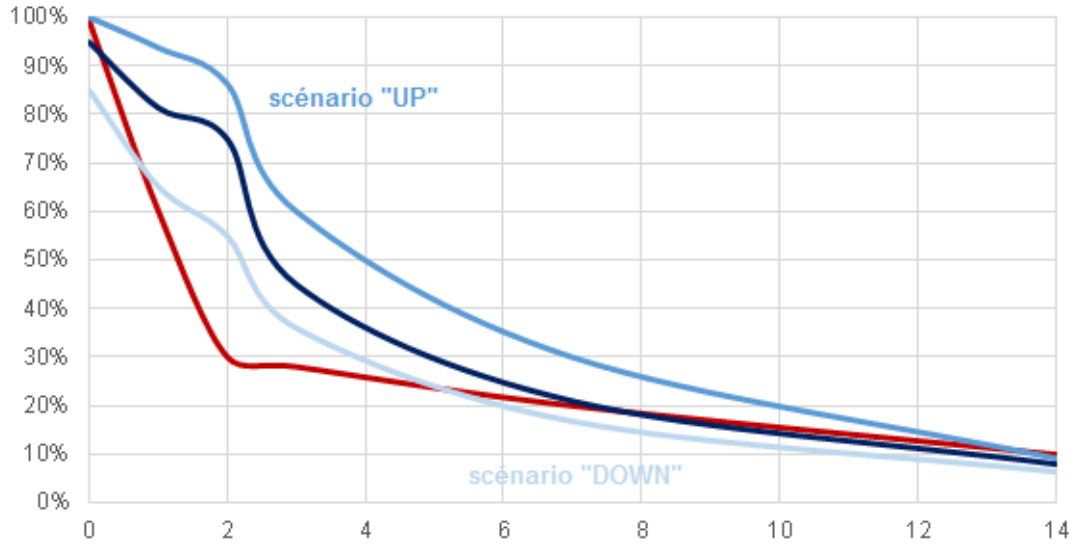


FIGURE 26 – Courbes des récupérations : scénarios standard, "*up*" et "*down*"

En ce qui concerne les hypothèses prises sur le rendement des différents secteurs d'activité pendant le Black-out, ces paramètres ont été modifiés de la façon suivante pour les scénarios "*up*" et "*down*" :

		Rendement pendant un BO		
Secteur d'activité	**Part de la VA**	Standard	"*up*"	"*down*"
Agriculture	0,20%	90%	80%	100%
Services	25,40%	60%	50%	70%
Finance	18,90%	50%	40%	60%
Industrie	55,50%	40%	30%	50%

Table 34 – Fonctionnement pendant le Black-out (vision "*up*" et "*down*")

Pour conclure, la sinistralité mesurée sur le scénario standard était de 44 012 394 EUR pour la perte d'exploitation. Les hypothèses de la vision pessimiste "*up*" résulte en une perte globale de 52 202 653 EUR soit près de + 20%. Pour le scénario "*down*", nous trouvons 38 911 544 EUR soit environ - 15%.

Ainsi nous pouvons conclure que la sensibilité du résultat aux différentes hypothèses n'est pas problématique dans l'approche par scénario puisque les visions pessimiste et optimiste restent dans le même ordre de grandeur que le modèle standard. Les paramètres peuvent ensuite être adaptés en fonction de l'appétence au risque et des volontés de protection en réassurance de la compagnie d'assurance concernée.

8 Application de la méthode "fréquence × coût" à un portefeuille d'assurance

Nous allons désormais présenter l'application de la modélisation "fréquence × coût" au portefeuille de garanties cyber présenté en partie précédente. À partir des caractéristiques de nos engagements (la taille de l'entreprise et de son secteur d'activité), nous pouvons générer aléatoirement une probabilité d'occurrence et une estimation de coût (par la génération d'une ampleur et d'un facteur d'aggravation, rendue possible par l'ajustement des lois statistiques) d'une violation de données potentielle. Ainsi, nous pourrons estimer une tarification par exposition pour une couverture cyber protégeant des violations de données.

8.1 Adaptation au marché français

Nous pouvons tout d'abord souligner que notre portefeuille est constitué de risques français. En effet, les statistiques descriptives de la base montrent que plus de 99% des engagements sont situés sur le territoire géographique français. Cependant, les paramètres déterminés dans la partie précédente est basée sur des données issues d'observation du marché américain. Pour pallier ce problème et adapter notre modèle aux spécificités de notre pays cible (ici le France), nous pouvons nous appuyer sur plusieurs études notamment les rapports "*Ponemon Institute : Cost of a Data Breach Study*" (2016, 2018 et 2019). Dans lequel sont comparées les violations par pays.

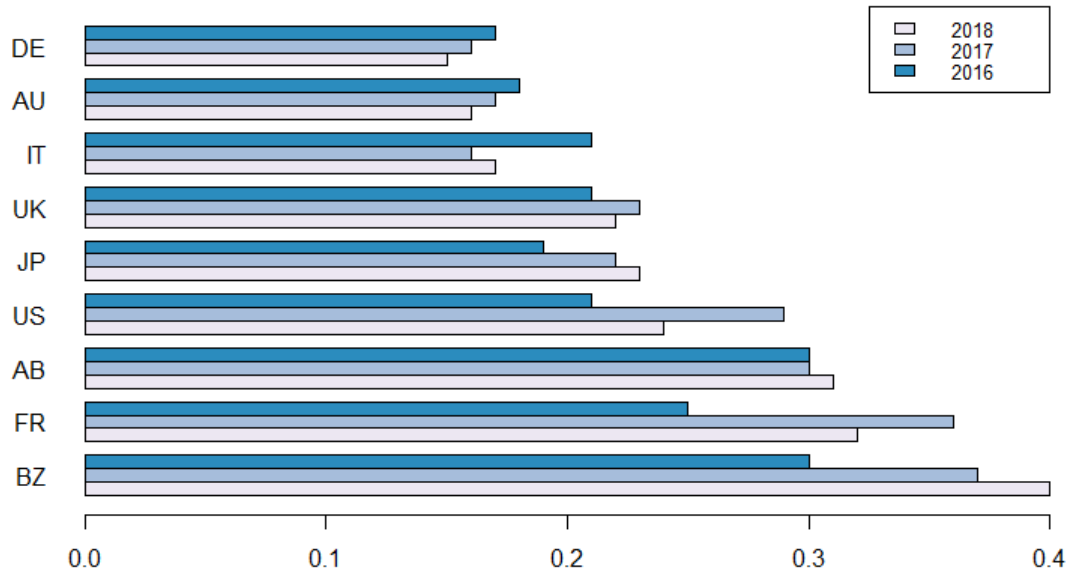


FIGURE 27 – Probabilité d'une violation de données [88] par pays

88. Sont considérés ici uniquement les vol de bases de plus de 10 000 enregistrements.

Nous créons donc un premier coefficient d'adaptation en ce qui concerne la fréquence des violations. Nous voyons que la probabilité des plus élevée en France, donc l'occurrence doit être amplifié. Après notre calcul sur l'historique présenté, nous obtenons un coefficient d'environ 115%. Ce chiffre peut être observé sur la figure 27 ci-dessus en comparant les barres "FR" (France) et "US" (États-Unis).

De même, mis à part le coût de la violation de données où nous avons utilisé des observations françaises, les paramètres de notre modèle ont été calculés sur des données américaines et nous devons donc procéder à un travail d'adaptation pour notre outil.Les mêmes études ont été analysées et nous pouvons tirer la conclusion suivante : pour la sévérité de la violation, en moyenne aux états-unis, une perte atteint environ 30 000 enregistrement pour approximativement 20% de moins en France. Ainsi nous avons déterminé notre deuxième coefficient d'adaptation qui sera donc de 80%.

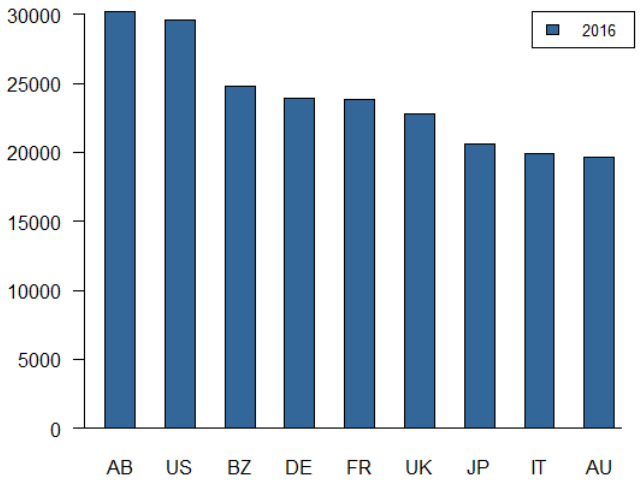


FIGURE 28 – Taille moyenne des violations déclarées en 2016 par pays [89]

Traduction de la perte brute en coût assurantiel

Enfin, nous devons distinguer le coût d'une donnée perdue pour une entreprise et le montant du remboursement provenant de l'engagement de la compagnie d'assurance responsable. En effet, toutes les pertes infligées par une violation informatique ne sont pas forcément assurables. L'étude de *IBM Security* publiée en 2019 nous présente la décomposition des coûts d'un enregistrement volé au cours d'une attaque cyber : plus des deux tiers des pertes sont couverts par les garanties affirmatives (principalement gestion de crise et responsabilité civile professionnelle). Mais certains dégâts ne sont pas protégés comme par exemple la perte de clients (non pas la perte d'activité) et les coûts dépensés pour les retenir ou en acquérir de nouveaux.

89. Source :"*Cost of a Data Breach Study*", Ponemon Institute 2016.

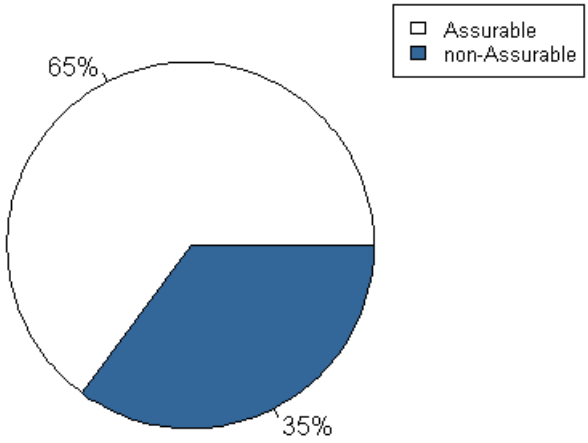


FIGURE 29 – Part de coût assurable dans les pertes financières d'une violation cyber

Ainsi, nous avons ajusté notre modélisation avec ce coefficient. Il n'est pas ici question de différence entre les marchés français et américain, mais bien de quels coûts sont assurés par notre portefeuille, et dans notre cas, il s'agit des pertes liées à la RCP, la gestion de crise, la perte d'exploitation, le dommage au bien et le *"Data and Software Loss"*[90].

Paramètre adapté	**Facteur d'adaptation**
Fréquence	115%
Nombre d'enregistrements	80%
Coût moyen unitaire[91]	100%
Coût assurable	65%

TABLE 35 – Récapitulatif des facteurs d'adaptation au marché français

Le tableau ci-dessus résume nos hypothèses d'adaptation au marché français. Nous pouvons à présent effectuer la tarification de notre portefeuille.

Application mathématique par la méthode de Monte Carlo

Nous allons effectuer cette modélisation en simulant la sinistralité annuelle un grand nombre de fois, à la méthode de Monte Carlo pour obtenir des résultats robustes[92]. Cette génération de l'ampleur de la perte de données se fait à partir de l'ajustement estimé lors de la création du modèle "fréquence × coût". Nous effectuerons 75 000 simulations. La partie suivante présente les résultats obtenus.

90. Il s'agit des polices qui couvrent notre portefeuille, voir page 47.
91. Le montant moyen unitaire considéré dans la construction du modèle est extrait d'une étude de l'institut *Ponemon*, concernant déjà le périmètre français. Aucune nécessité d'adapter cette valeurs.
92. La théorie de cette méthode est détaillée en Annexe P : "La Méthode de Monte Carlo".

8.2 Présentation des résultats

Partant des distributions paramétrées (fréquence, coût, sévérité) et des coefficients construits (adaptation au marché français, part assurable d'une donnée) dans ce chapitre, et en utilisant les méthodes décrites précédemment (génération aléatoire, méthode de Monte-Carlo), nous pouvons appliquer notre modèle au portefeuille. Ainsi, nous obtenons une perte annuelle globale, et en conséquence, par police. Ci-dessous, nous présentons des tableaux récapitulatifs des résultats.

Nb. Sim.	N	Ecart-type	Min.	Q. 25%	Moy.	Q. 75%	Max.
75 000	50 000	498 322	25 602 487	26 982 768	27 320 667	27 651 006	29 256 492

Table 36 – Présentation de la charge brute annuelle totale - Modèle "fréquence $\times$ coût"

Nb. Sim.	Ecart-type	Min.	Q. 25%	Moy.	Méd.	Q. 75%	Max.
75 000	9,97	512,0	539,7	546,4	546,4	553.0	585,1

Table 37 – Présentation de la charge brute annuelle par police - Modèle "fréquence $\times$ coût"

Nous pouvons donc voir que les résultats obtenus sont assez robustes. La volatilité est très faible. En effet, le coefficient de variation, mesure de dispersion, est à peine de :

$$c_\nu = \frac{\sigma}{\mu} = \frac{498\ 322}{27\ 320\ 667} = 1{,}82\%$$

Cela signifie que les sinistralités annuelles vont se ressembler et qu'il n'y a pas de pic de sinistralité à attendre, d'après nos hypothèses. En analysant les chiffres en eux-mêmes nous voyons une perte moyenne par cédante d'un peu plus de 500EUR. Ce montant représente un prix technique auquel il faudrait ajouter une marge de précaution et une prime commerciale pour pouvoir le comparer à ce qui est proposé chez les assureurs aujourd'hui. Ce chiffre est satisfaisant et se rapproche des montants trouvés sur le marché dans l'ordre de grandeur (plutôt le marché américain). Même si les tarifs appliqués par les compagnies d'assurance restent inférieurs à cela.

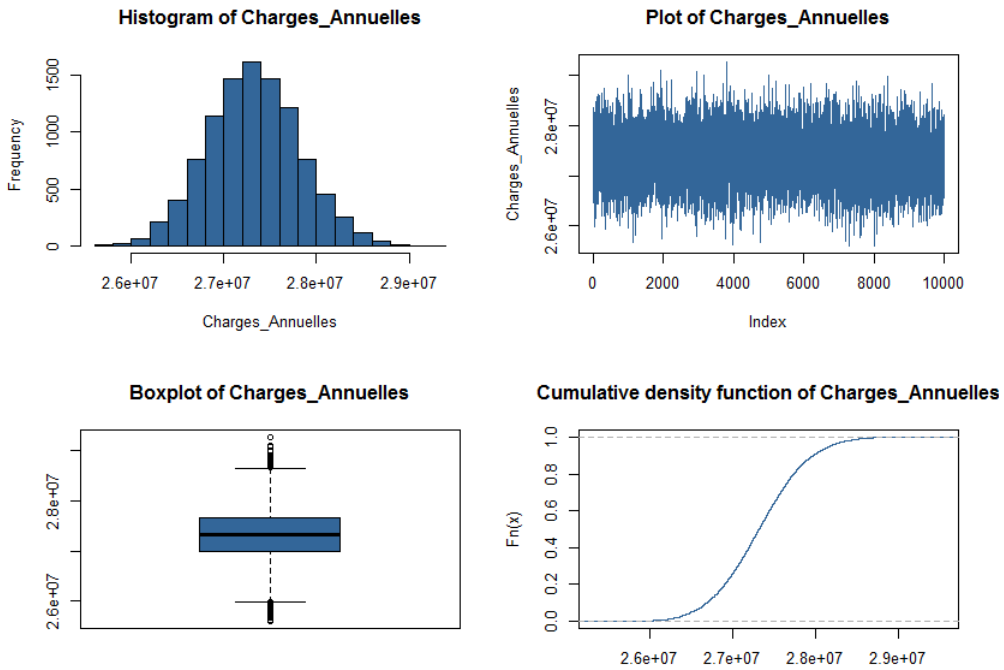


FIGURE 30 – Graphiques des charges annuelles brutes générées - modèle "fréquence × coût"

Les graphiques ci-dessus présentent les résultats de nos simulations. Nous voyons, comme décrit dans les tableaux, la faible volatilité et les quartiles rapprochés. Nous voyons également que les minimums et maximums ne sont pas des valeurs aberrantes, donc peu d'utilité de la réassurance pour ce risque là dans la gestion des situations extrêmes. Nous pouvons également préciser que ces résultats prennent en compte les limites des engagements de notre portefeuille, mais nous avons supposé qu'il n'y avait pas de franchise. En effet, la loi n'impose pas d'illimité comme en RC Automobile par exemple, et le risque cyber est peu maîtrisé donc les professionnels doivent imposer des limites.

8.3 Conclusions et limites sur le modèle "fréquence × coût"

En première partie de conclusion, nous pouvons dire d'une part que les résultats affichés par la modélisation sont cohérents. Ils s'approchent des montants retrouvés sur le marché des assurances cyber spécifiques. Il faut bien garder en tête que les polices d'assurances pour le risque informatiques incluent des limites assez basses. D'autre part, cette approche peut être mise en place assez facilement, sans avoir besoin de trop d'indication sur l'exposition de l'entreprise au risque cyber (serveurs utilisés, types de logiciels, sensibilisation des employés, etc.).

Cependant, nous pouvons évoquer différentes limites des chiffres obtenus. Tout d'abord, la construction entière du modèle est appuyée sur des bases de données a priori non exhaustives et pas très conséquentes en terme de taille. Le premier problème évoqué dans l'assurabilité de ce risque du manque de données disponibles est donc traduit en pratique dans notre tentative de tarifi-

cation. L'historique sélectionné est assez court (4ans) pour la fréquence. Les différentes hypothèses prises peuvent être discutables (adéquation des lois aléatoires, le coût moyen donné par l'institut *Ponemon*, la taille des bases endommagées, etc.). Les bases de données utilisées ne sont pas réglementaires donc pas forcément exhaustives. La méthodologie proposée était donc applicable (uniquement) pour le risque de violation de données ("*data breach*"), aux États-Unis, qui est le secteur où nous avons le plus d'information à disposition, et nous l'avons adaptée aux spécificités françaises.

D'autre part, dans la conception d'un modèle "fréquence × coût", il est important de remettre en cause l'hypothèse principale d'indépendance entre ces paramètres. Or, dans le cas du cyber, leur indépendance n'est pas évidente, comme nous avons pu le voir dans la description du marché. Nous pouvons également émettre une réserve quand à l'indépendance des attaques entre elles : une faille dans un système de défense pour une entreprise peut être également présente chez un concurrent. Ainsi un pirate peut profiter plusieurs fois d'une intrusion. De même que pour les vulnérabilités *0-day*, ce genre de scénario peut être imaginable pour une violation de données et doit être pris en compte. Ainsi, une limite à notre modèle serait la prise en compte de l'intégralité des variables explicatives : il manque des facteurs à notre modèle, dont notamment l'interconnexion ou la répartition géographique par exemple. D'autre part, l'absence de volatilité dans nos résultats est révélatrice de coefficients trop large et d'une granularité grossière, ce qui est problématique pour l'analyse des scénarios extrêmes. De plus, le modèle est construit et expérimenté sur une population relativement hétérogène, où la diversification dans le portefeuille permet d'obtenir des moyennes cohérentes. Il peut y avoir un biais de sélection adverse dans l'assurabilité du risque cyber, comme nous avons vu dans la partie 3.3, et donc que la population cherchant à s'assurer est en fait porteuse du plus gros risque (par exemple, les grandes entreprises financières ou pharmaceutiques). Pour conclure, nous pouvons indiqué l'absence de prise en compte du risque d'accumulation dans cette section. Manquement qui va tenter d'être comblé dans la partie suivante.

9 Nouveau modèle et risque d'accumulation

9.1 Prise en compte de l'interconnexion

Comme expliqué précédemment, nous allons prendre en compte de nouveaux facteurs plus propre au risque cyber. Nous allons essayer de tarifer la part de risque d'accumulation dans l'exposition des entreprises de notre portefeuille.

Nous nous penchons à présent sur un nouveau modèle d'appréhension du risque cyber : il s'agit d'un modèle marché. Dans cette approche, nous allons placer au centre de nos hypothèses l'importance de la prise en compte de l'interconnexion entre les entreprises. En effet, l'exposition aux différentes menaces cyber est partagée par les potentielles victimes. Le partage des ressources, les serveurs en réseau et les systèmes d'exploitation, étant souvent identiques voire similaires (en fonction des secteurs d'activité notamment) constitue une amplification des expositions. Pour l'ensemble des risques informatiques, il est intéressant de réaliser qu'une vulnérabilité dans un système de défense permet souvent plusieurs entrées. Par exemple, comme nous l'avons vu précédemment avec les vulnérabilité *0-day*[93], une faille dans un logiciel comme Windows peut être exploitée pour voler des données chez plusieurs entreprises dans un laps de temps très réduit.

Ainsi, nous allons pouvoir challenger notre modèle "fréquence $\times$ coût" en insérant cette fois ci dans le modèle la corrélation entre les probabilités d'occurrences des attaques numériques. Sans nous focaliser uniquement sur la violation de données, nous allons essayer de voir l'impact de la prise en compte de l'interconnexion dans les modélisations actuarielles des risques informatiques [94].

Tout d'abord, le système d'exploitation (ou "OS pour" *"Operating System"* en anglais) d'un ordinateur ou d'une machine connectée est l'ensemble des programmes régissant son fonctionnement : il s'agit des mécanismes dirigeant l'utilisation des ressources et des logiciels d'exécution des instructions. Il gère les processeurs et la mémoire vive de l'ordinateur, permet l'utilisation de périphériques et traite les commandes de l'utilisateur. Les OS les plus connus sont Windows (de Microsoft), MAC OS (de Apple) ou encore Android ou iOS pour les smartphones. En ce qui concerne notre problème, ces OS sont très souvent visés par des attaques cyber. Or, le quasi-monopole de Windows et la domination de seulement quelques fournisseurs impliquent que la plupart des entreprises utilisent les mêmes OS et donc sont exposées aux mêmes menaces. D'après les chiffres du graphiques ci-dessous, une faille chez Microsoft pourrait impacter jusqu'à 90% du marché.

93. Voir partie 1.2, page 19 : une vulnérabilité *0-day* est une attaque cyber exploitant une faille numérique encore inconnue du logiciel vendeur.

94. Source : "Les chiffres du marché cyber", sdnet.fr 2019.

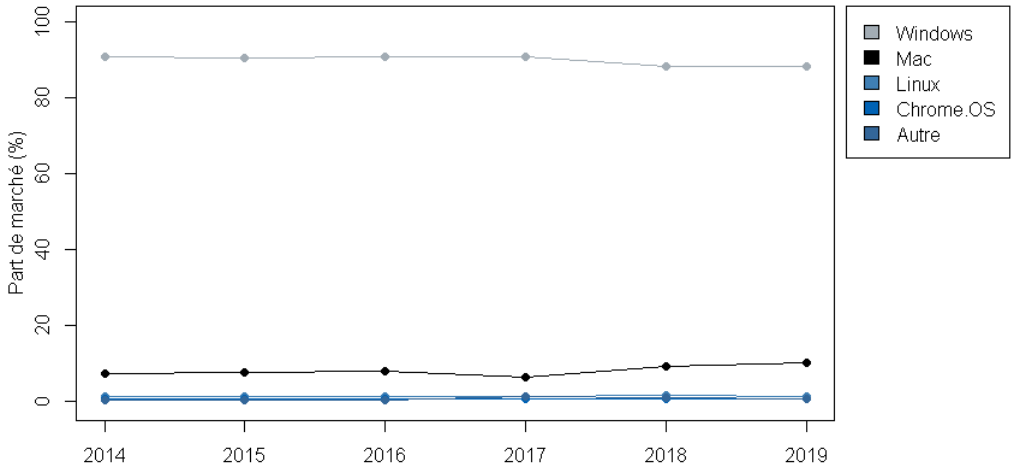


FIGURE 31 – Évolution des parts de marché des fournisseurs de systèmes d'exploitation

Nous pouvons de plus observer sur le graphique de la figure 31 que les tendances n'évoluent pas vraiment et que la domination semble pérenne pour cette poignée d'acteurs. Nous pouvons à présent nous pencher sur le marché des fournisseurs de logiciels de sécurité informatique. En effet, ces vendeurs proposent des outils d'analyse et de nettoyage des dossiers et de la mémoire d'un ordinateur. Le but étant de protéger les machines en évitant toute introduction parasite ou virale. L'enjeu du choix et de la performance d'un logiciel de sécurisation informatique dans la gestion du risque cyber est prédominant. Il est essentiel d'être bien protégé techniquement pour réduire son exposition aux piratages. Or, nous observons sur le marché la domination des géant de la sécurité numérique, comme Symantec ou MacAfee, qui possèdent respectivement environ 18% et 12% du marché. Ainsi, Or, de même que pour les systèmes d'exploitation mais dans une moindre mesure, nous sommes confrontés au même problème d'interconnexion.

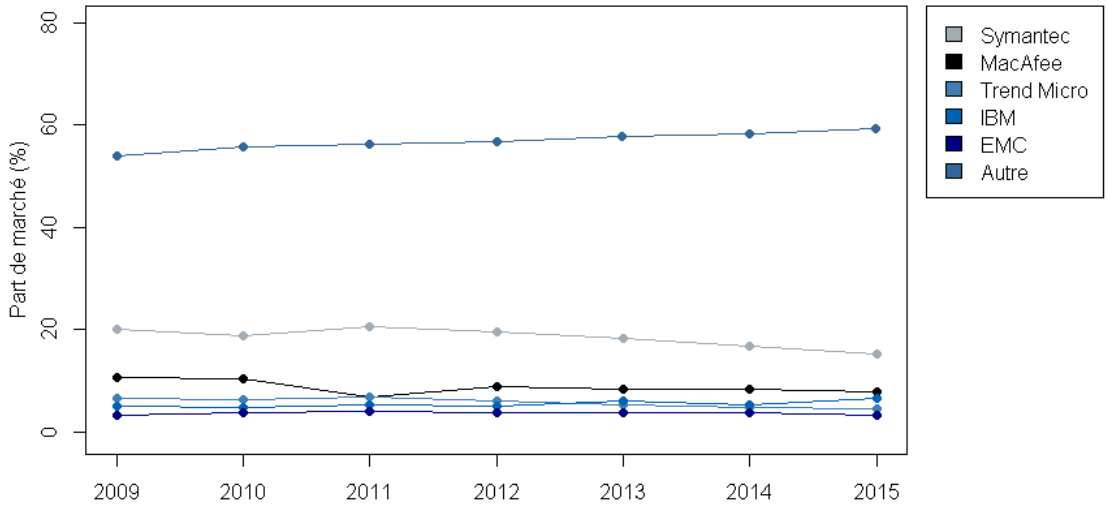


FIGURE 32 – Évolution des parts de marché des vendeurs de logiciels de sécurité

La tendance observée sur le graphique des évolutions annuelles est plus optimiste que la pré-

cédente puisque nous voyons que la catégorie "autre" est majoritaire et semble continuer à prendre de l'importance. Cela implique une meilleure distribution du marché entre les acteurs et donc une interconnexion limitée entre les risques. Les expositions sont tout de même amplifiées par le fait que les logiciels de sécurité proviennent principalement des quelques mêmes fournisseurs. Il faut prendre cela en compte dans nos modèles d'appréhension du risque informatique.

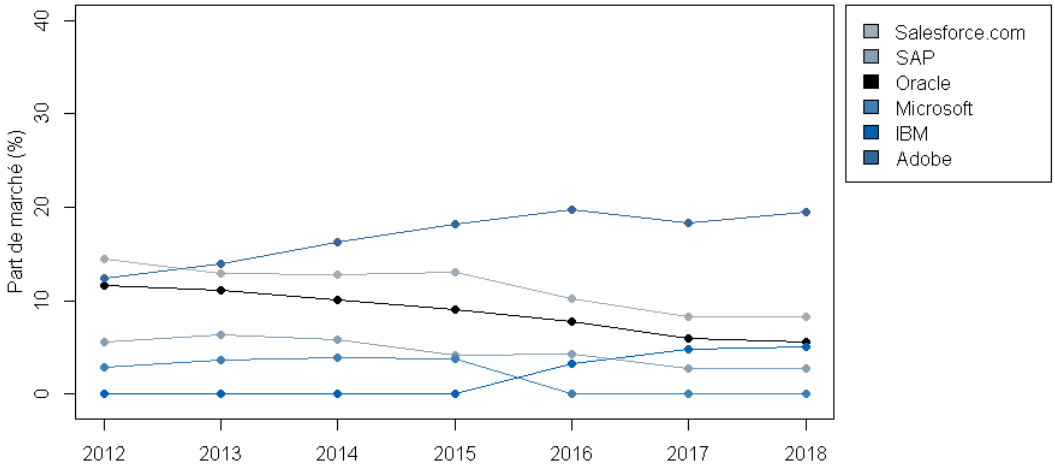


FIGURE 33 – Évolution des parts de marché des éditeurs de logiciels CRM

Les logiciels CRM [95] sont les outils de gestion des relations professionnelles pour une entreprise. Il s'agit de processus centralisant les échanges et interactions d'une firme et ses fournisseurs et clients. Ces programmes voient passer beaucoup d'informations clés des entreprises et de leurs partenaires. Ce sont les logiciels les plus visés, d'une part parce qu'ils abritent beaucoup de bases de données sensibles et confidentielles, et d'autre part parce qu'ils sont des pièces maîtresses dans l'activité professionnelle de leur propriétaire. Une nouvelle fois, nous voyons l'immense domination de quelques entreprises (dont Salesforce.com, SAP AG ou encore Oracle). Nous pouvons ajouter que les fournisseurs de CRM peuvent être répartis en plusieurs catégories et que chaque catégorie a un leader qui se concentre sur des domaines professionnels (comme la santé, ou le bâtiment par exemple). Ainsi, en plus de souffrir d'un manque de diversification de manière générale, les interconnexions sont encore plus forte intra-secteur d'activité ce qui augmente l'exposition commune.

Enfin, pour finir d'illustrer l'importance de la prise en compte de la corrélation entre les risques informatiques des entreprises, nous pouvons nous pencher sur les offres de dispositifs de connexion. En effet, les serveurs informatiques permettent l'accès à internet et accueil les dispositifs d'échange par *e-mail*. Les serveurs peuvent également abriter des bases de données importantes et permettent un accès au *cloud* [96].

95. *Customer relationship management.*
96. *"Cloud"* ou "nuage" en français : il s'agit de la technologie informatique permettant de stocker et d'exploiter des bases de données via des serveurs distants. Source : Wikipedia, 2019.

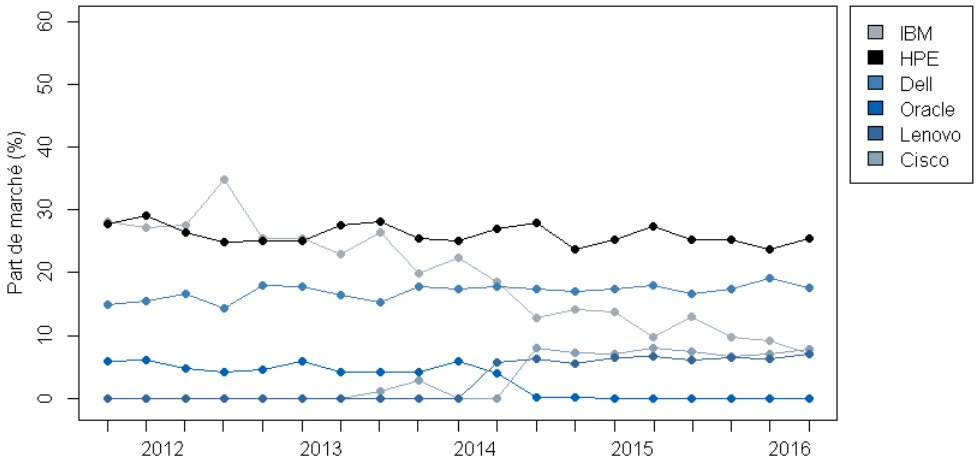


FIGURE 34 – Évolution trimestrielle des parts de marché des principaux serveurs

Nous observons ci-dessus l'évolution par trimestre des parts de marché en terme de chiffre d'affaire des entreprises fournisseurs de serveurs. Nous pouvons une fois de plus noter la supériorité de quelques entités sur leur concurrence.

Nous comprenons donc l'importance de la connaissance de la branche informatique dans la compréhension du risque informatique. En effet, l'analyse de l'historique ne suffit pas pour comprendre réellement l'exposition des entreprises et les pertes potentielles assurées. Il faut un diagnostic profond du réseau et des mécanismes informatiques pour mesurer la performance des systèmes de protection et la sensibilité des données possédées. Les actuaires (et gestionnaires du risque de manière générale) ont recours à des experts cyber de l'informatique. Certaines modélisations voient le jour, issue de la collaboration entre compagnie d'assurance et les leaders en matière de sécurité numérique (comme Symantec par exemple). L'un des exemples de modèle ayant vu le jour suite à un véritable diagnostic en profondeur et une collaboration entre les experts des réseaux numériques et les actuaires est l'approche par *cyber Kill Chain* probabilisée [97]. Cette méthode propose une probabilité de réussite à chaque étape d'une attaque informatique en fonction des moyens de protection de l'entreprise cible.

9.2 Considérer le risque d'accumulation : résultats, conclusions et limites

Nous avons donc inclus nos hypothèses de prise en compte d'interconnexions entre les risques du portefeuille présentées dans la section précédente. Cette partie se consacre donc à la présentation des résultats, particulièrement des nouvelles informations sur la sinistralité, apparues avec la prise en compte du partage des expositions. Comme évoqué plusieurs fois dans ce mémoire, le manque de données sur ces risques rend difficile son étude : il est délicat de valider nos lois avec les indicateurs des méthodes classiques (erreur quadratique moyenne ou erreur absolue) ou par étude du compromis entre biais et variance. Nous pouvons en revanche les comparer avec ce que l'on

97. Voir Annexe Q : "La *kill chain* probabilisée".

trouve sur le marché.

	Perte annuelle	**Perte annuelle par entreprise**
Perte moyenne (EUR)	31 937 048	638

Table 38 – Montant de la perte annuelle moyenne (en EUR)

Le tableau ci-dessus présente les pertes annuelles moyennes issues de nos simulations. Nous pouvons tout d'abord remarquer que la sinistralité estimée par cette modélisation est supérieure à celle de l'approche sans l'interconnexion, ce qui semble cohérent. Il peut être intéressant à présent de regarder les quantiles de distribution des pertes pour étudier les périodes de retour et analyser les probabilités d'atteinte de différents seuils de sinistralité.

Période de retour	**Perte (EUR)**
20 ans (0,05)	35 939 927
50 ans (0,02)	38 657 856
100 ans (0,01)	41 872 380
200 ans (0,005)	45 049 876
250 ans (0,004)	45 581 194
500 ans (0,002)	47 727 111
1 000 ans (0,001)	50 965 451

Table 39 – Montant de la perte (en EUR) par période de retour

Nous remarquons que la sinistralité (toujours nettement supérieure à celle affichée par le modèle "fréquence $\times$ coût") ne contient pas de grands pics, et donc les récupération à 500 ou 1 000 ans restent dans le même ordre de grandeur. Nous pouvons également mentionner ici l'intérêt de la protection par la réassurance de ce genre de risque. Au vu du profil des pertes et des différents quantiles présentés, nous pourrions imaginer des couvertures en excédent de sinistre par tranches successives pour protéger le résultat de compagnie d'assurance. Il devrait s'agir d'un programme avec une portée importante.

Dans les résultats à afficher après une étude de perte sur un portefeuille cyber, il peut être intéressant d'analyser l'empreinte du risque en question. C'est-à-dire, comprendre combien d'entreprise ont été touchées et de faire des focus sur ces victimes. Le tableau ci-dessous présente le nombre moyen d'entreprises impactées, par logiciel attaqué, pour les plus gros contributeurs de sinistralité. Il s'agit de moyenne par simulations de violation de données.

Logiciel cible	Type de perte	Nombre moyen d'entreprises impactées
Lenovo Server	Serveur	2 953
Hewlett Server (HPE)	Serveur	3 291
Windows (Microsoft)	Système d'opération	6 253
Debian (Linux)	Système d'opération	2 555
Microsoft Outlook	Application	695

Table 40 – Empreinte moyenne de la perte dûe à l'interconnexion

Nous pouvons ainsi constater que dans les 50 000 risques singuliers que comporte notre portefeuille, les interconnexions sont importantes. En effet, nous voyons que certaines failles sont exploitées pour endommager plusieurs milliers d'entreprises. Ces logiciels sont responsables de pertes importantes et le fait qu'ils soient communs à plusieurs établissements, amplifie grandement l'exposition totale pour la compagnie d'assurance responsable de la couverture de ces derniers.

Conclusions et limites

L'intérêt de cette dernière approche est de prendre en compte le fait que la menace cyber se développe sous deux formes distinctes : au travers d'un risque individuel à chaque assuré (chaque entreprise) ou bien sous forme de risque dit "d'accumulation" qui serait donc associé à un potentiel défaut systémique (par exemple du *cloud provider* ou du serveur). Ces ajouts permettent l'analyse des composants uniques de chaque type de risque afin de répliquer le comportement des entreprises face à la menace potentielle. Des hypothèses ont été faites pour coller au monde réel et pour projeter les calculs de pertes et l'application des scénarios de catastrophe d'attaque cyber, dans notre cas pour une violation de données.

Le modèle prend en compte les caractéristiques spécifiques de chaque type de risque en utilisant des hypothèses et des méthodologies spécifiques qui représentent au mieux leur comportement attendu dans la réalité. Ces hypothèses, basées sur l'étude statistique présentée dans la première section aident à piloter les calculs des pertes projetées potentielles et servent de base à l'analyse de scénario de sinistre. Les risques individuels et les risques d'accumulation ont des ensembles respectifs de types d'évènements. Pour ces évènements, les observations relatives aux données empiriques et aux contributions d'experts servent de base à un modèle statistique basé sur leur fréquence (fréquence de l'évènement) et leur gravité (pertes associées à l'évènement) : modèle "fréquence $\times$ coût". Le modèle de fréquence est ensuite utilisé pour simuler les occurrences annuelles d'évènements de l'ensemble d'évènement. Pour chaque évènement simulé, les pertes de chaque société touchée sont estimées à l'aide du modèle de gravité. Les informations de police associées sont ensuite superposées pour calculer les pertes assurées pour la sociétés, ces pertes au niveau de la police étant ensuite combinées dans l'ensemble du portefeuille pour obtenir le bilan pour la compagnie d'assurance.

10 Comparaisons, conclusions, limites et ouvertures

Cette section est consacrée à l'analyse des résultats et une comparaison des différentes approches proposées dans le dernier chapitre. Nous reviendrons rapidement sur les modèles, les hypothèses importantes et leurs niveaux de crédibilité, avant de conclure sur l'utilisation qui peut en être faite. Nous nous pencherons également sur les difficultés que nous avons rencontrées et les menaces identifiées pour le futur, et l'adaptation potentielle des mesures de l'exposition au risque cyber.

Comparaison des modèles sur le *data breach*

En terme de comparaison des résultats, l'approche par scénario n'étant pas une approche à but de tarification à proprement parler, et ne traitant pas du risque de violation de données, nous ne pouvons les mesurer aux autres modèles. Cependant, les approches avec et sans prise en compte de l'interconnexion peuvent être enrichissante à comparer. Nous pouvons remarquer la part de risque d'accumulation dans le nouveau modèle en faisant la différence avec les résultats obtenu avant la prise en compte des interconnexions. Nous allons simplement comparer les moyennes pour voir une idée de la part concernée : 31 937 048 - 27 320 667 = 4 616 381 EUR, soit :

$$\frac{31\ 937\ 048}{27\ 320\ 667} - 1 = 16,9\%$$

Nous pouvons ainsi illustrer l'importance de la prise en compte de l'interconnexion puisque d'après notre modélisation, cette dernière serait responsable de $16,9\%$ de la sinistralité, en moyenne. D'autre part, le graphique ci-dessous nous permet de comparer les primes individuelles annuelles estimées de nos modèles. La comparaison des sinistralités brutes étant rendues difficiles par les écarts nominaux des montants, nous illustrons l'impact de la prise en compte des interconnexions avec la prime pure (calculée comme le risque totale porté par le portefeuille divisé par le nombre d'engagement, ici 50 000).

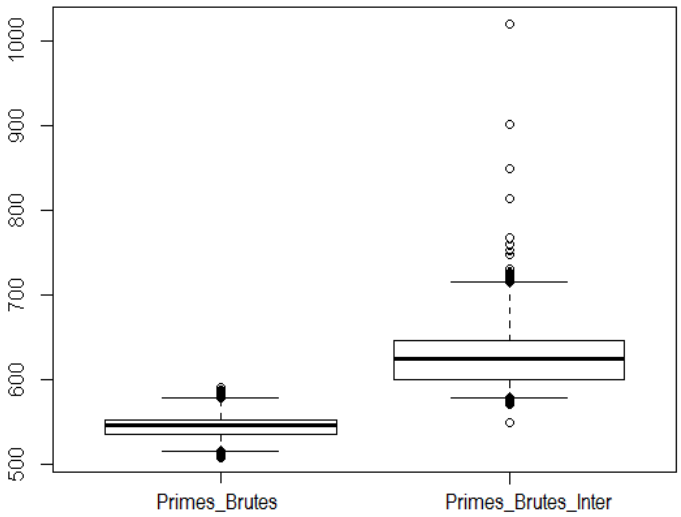


FIGURE 35 – *Boxplot* de comparaison des primes

Ainsi nous pouvons noter également qu'en plus d'influer sur le montant moyen (+16,9 %), l'inclusion des interconnexions fait évoluer la distribution de la sinistralité, et donc de la prime technique de 546 EUR à 638 EUR. Rappelons tout de même que d'après nos hypothèses de calculs, ces montants devraient être ventilés sur le portefeuille à partir des spécificités de chaque engagement, notamment les limites des contrats mais aussi la taille de l'entreprise couverte et son secteur d'activité. Notre modélisation ayant plutôt pour objectif de mesurer l'exposition totale du portefeuille, une telle précision n'est pas pertinente.

Des difficultés à construire et exploiter des modèles cyber

Nous avons tout d'abord effectué une approche par scénario : cette méthode permet d'estimer l'exposition générale au risque cyber pour un portefeuille d'assurance. En nous appuyant sur des travaux similaires menés au Japon et aux États-Unis, nous avons analysé les particularités et la solidité du réseau de distribution d'énergie d'Île de France. Nous avons ainsi pu cibler les différentes zones sensibles et potentiellement attaquables. Nous avons ainsi dresser une liste des atouts et points faibles de ce réseau pour imaginer un scénario de destruction puis de réhabilitation, et notamment une courbe de restauration. La sinistralité assurable estimée de ce scénario s'élève à plus de 30m EUR, principalement de la perte d'exploitation. Ce montant est comparable aux expositions portés par un portefeuille similaire pour du risque catastrophe naturel, hors les primes ne sont pas à la même échelle. Nous avons émis quelques réserves sur ce chiffre, mais son ordre de grandeur nous permet de confirmer l'importance de ce "nouveau" risque dans le paysage des assurances.

Nous avons pu voir la diversité des types de pertes observées et l'ampleur de la sinistralité générée : une incidence de cette gravité est peu probable, mais nous pensons qu'elle est représentative du type d'événements extrêmes que les assureurs devraient évaluer afin de comprendre les

expositions potentielles. Une des particularités principales du risque cyber est le large éventail de pertes possibles : illustré par ce scénario, nous voyons que le risque informatique représente un péril qui pourrait entraîner des pertes dans de multiples secteurs de l'économie, et donc déclencher des demandes d'indemnisations assurantielles pour pratiquement tout type de police. Néanmoins, la probabilité et l'impact des événements graves restent soumis à beaucoup d'incertitude. En effet, le manque de connaissance et de données est un véritable frein dans le développement de modèles précis.

Nous avons ensuite exploité plusieurs bases de données de diverses provenances [98] afin de proposer une approche plus mathématique. Nous avons construit un modèle "fréquence $\times$ coût" en prenant différentes hypothèses, dans le but de tarifer une protection assurantielle spécifique contre la violation de données. Le coût généré en deux temps par la taille de la base pénétrée (par une loi log-logistique) et le coût moyen unitaire (par l'étude du rapport du *Ponemon Institute*) combiné à la fréquence d'occurence paramétrée sur une loi Binomiale Négative nous a permis d'effectuer des simulations par la méthode de Monte Carlo pour obtenir une sinistralité globale annuelle moyenne d'environ 27,9m EUR.

Nous arrivons ainsi dans un premier lieu à une prime technique moyenne de 546 EUR (simplement la sinistralité totale distribuée sur les 50 000 engagements du portefeuilles). Ce montant semble relativement cohérent [99], et nous permet de confirmer la pertinence de notre travail et des hypothèses dans leur ensemble. Après la prise en compte de l'interconnexion pour l'estimation de l'exposition au risque d'accumulation pour la menace cyber, nous obtenons un prix pur de 638 EUR par entité sur notre portefeuille, soit une augmentation de +16,9% dûe uniquement à l'introduction du risque de cumul. Ces approches sont comparables dans les risques couverts par les assurances étudiées, et nous voyons qu'il existe une cohérence entre les travaux (la prise en compte des interconnexions augmente le prix).

Bien que les résultats présentés soient satisfaisants, il est nécessaire d'améliorer la qualité des données disponibles et de poursuivre le développement de modélisations probabilistes. Le partage des données de sinistralité cyber est un problème complexe, mais cela pourrait être une des clés dans la construction de solution d'assurance. La nature systémique et évolutive du risque cyber représente un défi pour l'économie mondiale : rendant quasiment impossible l'emploi des méthodes "classiques" de mesure de l'exposition, les actuaires doivent s'adapter et faire preuve de créativité pour appréhender cette menace.

98. Aon et RBS (base interne), SAS OpRisk Global Data (demandée au service client SAS), Ponemon Institute (téléchargée sur internet), etc.)

99. Cohérent, même si un peu plus cher que le marché, sans compter qu'il est hors franchise et exclusion.

Lien avec le *Ransomware*

En guise de rapide ouverture, il est intéressant d'évoquer que la violation de données est factuellement très similaire au *ransomware*. Il s'agit, comme défini dans la partie 1.2, d'un logiciel malveillant qui "prend en otage" les informations de la victime et exige le paiement d'une rançon en échange de la libération de ces dernières [100]. Il n'existe à l'heure actuelle aucun modèle performant pour mesurer l'exposition au risque cyber de *ransomware*. Il est intéressant de noter qu'un modèle "fréquence × coût" sur le *data breach* pourrait être adapté pour le risque de *ransomware*.

D'une part, cette transaction monétaire effectuée par l'entreprise affectée est souvent demandée en Bitcoin, pour sa qualité d'intraçabilité notamment. Pour plus de précision, nous pourrions alors imaginer un modèle où le coût serait lié aux variations du cours de cryptomonnaies. Ainsi, en modifiant la sévérité à partir du cours du Bitcoin et la fréquence à partir d'une étude d'occurrence : on estime aujourd'hui qu'il y a environ 3 fois plus de *ransomware* que de vols de données [101]. Nous pourrions ainsi impacter la distribution de fréquence avec cette information et donc avoir un modèle fonctionnel pour le risque cyber de *ransomware*.

FIGURE 36 – Cours du Bitcoin depuis novembre 2018 (en €)

Si on se concentre plus précisément sur l'utilisation du *Bitcoin*, les spécialistes de *Cybersecurity Ventures* prévoient que d'ici 2021, plus de 70 % de toutes les transactions en cryptomonnaies seront destinées à des activités illégales, alors que les estimations actuelles vont de 20% (des cinq principales cryptomonnaies) à près de 50 % (du Bitcoin). Selon une étude publiée par l'Université de Sydney en Australie environ 76Md USD d'activités illégales par an impliquent le *Bitcoin*, ce qui est proche de l'échelle des marchés américain et européen des drogues dures [10].

100. Ce processus est exécuté au moyen du chiffrage et du déchiffrage des données interceptées. L'interception en question implique très souvent des méthodes de "*phishing*" (ou "hameçonnage") pour piéger les entreprises.
101. Source : Hosting Tribunal (*hostingtribunal.com*), 2018

Les menaces identifiées pour le futur

Le risque cyber est, comme nous l'avons étudié tout au long de cette étude, une menace complexe, qui se renouvelle perpétuellement et dont les caractéristiques varient, avec le temps, la géographie, mais également en fonction de la cible (individuelle ou professionnelle) ou de l'attaquant. Nous cherchons dans cet ultime paragraphe à identifier les dangers naissants qui auraient une influence sur le risque informatique.

Nous pouvons citer en premier lieu le développement du marché des objets connectés et l'apparition de la 5G : de nouvelles vulnérabilités vont apparaître avec la puissance de ces débits. La capacité de sauvegarde et de transmission de données en grands volumes par les *cloud* offrira de nouvelles cibles.

D'autre part, le développement des intelligences artificielles (IA) représente également un danger : par la corruption des algorithme d'IA, ou leur utilisation dans la création (ou l'amélioration) d'attaques informatiques. Les IA auront probablement une part importante dans le quotidien d'ici quelques années (décennies) et nous devrons donc les gérer avec précautions.

Enfin, nous pouvons identifier une infection des *Supply Chain* (ou "chaîne logistique") comme un risque grandissant : par exemple, on peut imaginer le remplacement d'une mise à jour système par une mise à jour malveillante avant d'être envoyée aux millions d'utilisateurs du logiciel, ouvrant ainsi un grand nombre de vulnérabilité avant d'être identifiée.

Conclusion

L'exposition à la menace cyber représente aujourd'hui un enjeu immense pour les entreprises qui tentent de se protéger en se tournant notamment vers les assureurs afin de transférer leur risque. Le défi de la modélisation du caractère systémique de ce dernier est l'une des problématiques majeures pour le marché assurantiel.

Ce mémoire avait pour ambition de proposer une présentation complète du risque informatique en commençant par le définir et décrire son environnement. Nous avons pu constater que le marché français, en retard sur celui des État-Unis notamment, pesait tout de même plusieurs milliards de dollars et que les principaux acteurs développaient leurs offres au fil des années, pour répondre à la demande grandissante. Les types de pertes sont variés, et les motivations des acteurs également, ce qui fait du risque cyber une menace difficile à appréhender. Par le large éventail d'outils disponibles et la dépendance grandissante des entreprises et des particuliers aux machines connectées, le risque évolue vite et très fortement. A la survenance d'incident cyber, s'est ajoutée la mise en place d'un cadre réglementaire pour ce risque, visant à protéger les particuliers et les entreprises.

Les difficultés à proposer des solutions adaptées en terme de protection et de modélisation par les professionnels de l'assurance, ainsi que la réticence des acteurs à transférer leur exposition nous a poussé à nous questionner ensuite sur l'assurabilité du risque cyber. En nous appuyant sur les travaux de Berliner , nous avons étudié les critères sociétaux, légaux et mathématiques. Si la conformité aux valeurs de société et aux restrictions légales n'est pas assurée (à cause d'un fort aléa moral et de l'intraçabilité des attaques cyber principalement), elle ne vient pas remettre en question l'assurabilité du risque informatique. Les critères de marché, particulièrement en ce qui concerne les couvertures, présentent une limite : l'exposition est immense (comme notre dépendance aux ordinateurs), et la nature de la menace informatique trop complexe pour que les limites fixées soient appropriées à sa gestion. De plus, l'hypothèse du caractère aléatoire des pertes, et donc d'indépendance des pertes n'est pas suffisamment respectée dans le cas du risque cyber. Enfin, si les autres critères actuariels sont plutôt bien remplis, l'asymétrie d'information est de trop grande ampleur pour pouvoir être négligeable : l'aléa moral et la sélection adverse créent un biais trop important pour confirmer l'assurabilité du danger informatique. Nous avons traduit ces limites avec l'offre que l'on trouve sur le marché (en présentant les grandes lignes) : existante parce que les critères sociétaux et légaux sont respectés, mais pas attrayante à cause des restrictions économiques dues aux restrictions mathématiques de gestion de ce risque : les limites de garanties sont trop faibles et les franchises trop élevées.

La modélisation de la menace informatique est donc un véritable défi. Les principales difficultés proviennent du manque de données, du caractère évolutif du risque, de l'exposition silencieuse et

enfin du danger des cumuls pour un évènement cyber. Pour expliquer cela et tenter d'y remédier la deuxième partie propose la construction de modèles actuariels d'appréhension du risque cyber. En premier lieu, à l'instar des Lloyd's, nous avons proposé une modélisation par la création d'un scénario "Black-out Île-de-France", une perturbation informatique sur le réseau de distribution d'énergie en région parisienne. Les résultats affichés sont satisfaisant et permettent de mesurer l'exposition d'un portefeuille de garanties, mais traduisent cependant la complexité de la prédiction des pertes cyber. D'autre part, nous avons paramétré un modèle historique "fréquence $\times$ coût" sur le risque de *data breach*. Son application à un portefeuille de polices cyber spécifiques permet la mesure de l'exposition et prend en compte les spécificités du marché français. Nous pouvons tout de même constater que les hypothèses prises sont lourdes, et que les résultats ne sont pas complètement convaincants.

Nous concluons notre étude en introduisant la mesure des interconnexions dans les calculs d'exposition. En effet, de par le manque de données, l'évolutivité rapide et les risques de cumuls, les actuaires sont en difficulté pour proposer une bonne gestion de cette exposition et ont besoin de l'expertise d'informaticiens pour effectuer un scan du réseau internet et estimer régulièrement les vulnérabilités auxquels leur portefeuille est exposé.

Pour conclure, nous pouvons affirmer que le marché du cyber en France est encore appelé à se développer et les outils vont continuer à se préciser. Le commerce potentiel et la volonté du gouvernement vont pousser le développement de la compréhension et de la gestion de cette menace. Bien que l'appréhension en soit complexe, le marché de l'assurance à le potentiel pour soulager les entreprises face à ce risque. Mais les limites de son assurabilité et les difficultés de tarification du risque cyber demeurent de véritables problématiques dans la création de produits d'assurance adaptés et l'utilisation de méthodes classiques de modélisation.

Glossaire

ACPR Autorité de Contrôle Prudentiel et de Régulation
ANSSI Agence Nationale de Sécurité des Systèmes d'Information
BI Business Interruption
BO Black-out
CEPD Contrôleur Européen de la Protection des Données
CIL Correspondant Informatique et Liberté
CNIL Comission Nationale de l'Informatique et des Libertés
CPP Concurrence pure et parfaite
DDoS Denial of Service
DINC Dommage immatériel non-consécutifs
DSP Directive sur les Services de Paiement
EIOPA Autorité Européennes des assurances et des pensions professionnelles
ENISA Agence Européenne de sécurité de l'information et des réseaux
GEV Generalized Extreme Value
GLM Generalized Linear Model
IARD Incendie, Accident et Risque Divers
IPC Indice des prix à la consommation
ISO Organisation Internationale de Normalisation
KYC Know Your Customer
LGN Loi des grands nombres
LPM Loi Française de Programmation Militaire
MRH Multi-risque Habitation
NAICS North American Industry Classification System
NIS Network and Information Security
OIV Organismes d'Importance Vitale
PCI DSS Payment Card Industry Data Security Standard
PE Perte d'exploitation
PIB Produit intérieur brut
PSSI Politique de Sécrutié des Systèmes d'Information
RC Responsabilité Civile
RCP Responsabilité Civile Professionnels
RGPD Règlement Général sur la Protection des Données
RSSI Responsable de la Sécurité des Systèmes d'Information
RTE Réseau de Transport d'Electricité
RTS Standards Techniques Règlementaires
SAIDI System Average Interruption Duration Index
SAIFI System Average Interruption Frequency Index
SGDSN Secrétatiat général de la Défense et de la Sécurité Nationale
SIIV Systèmes d'Information d'Importance Vitale
SMSI Système de gestion de la sécurité de l'information
SNCF Société Nationale de Chemin de Fer Français
TVE Théorie des valeurs extrêmes
UE Union Européenne
VA Valeur Ajoutée
VA Variable Aléatoire
VPN Virtual Private Network
WEC World Economic Council

Table des figures

Liste des tableaux

Annexe A : Quelques exemples marquants

"NotPetya" : Il s'agit probablement de l'attaque cyber la plus célèbre de l'histoire moderne. Le vecteur initial de propagation de ce ver informatique était en Ukraine, qui se trouvait être la cible initiale du piratage. Il s'agit du logiciel de paiement de taxe *MeDoc*, victime via une mise à jour automatique durant laquelle le *ransomware* extrait les informations d'identifications des administrateurs. Avec ces droits élevés, le logiciel peut voler des mots de passe locaux en utilisant des outils de type MimiKatz [102] par exemple, afin d'injecter du code malveillant sur les machines connectées en réseau. La mise en place d'extraction des informations d'identification a été rendue possible par l'exploitation d'une faille de la sécurité Windows [103], erreur qui avait déjà été corrigée par Microsoft. Avec l'accès administrateur, l'attaque a consisté en un grand chiffrement des tables et fichiers du système, qui va de pair avec une demande de rançon pour libérer les données piratées. Lors de son apparition en 2017 [104], on pense qu'il s'agit du fameux *ransomware* "Petya" [105] mais il n'en est rien, ce nouveau danger est différent et plus élaboré, il est donc ironiquement baptisé NotPetya. Parmi les victimes, on compte de nombreuses entreprises comme la SNCF, Saint-Gobain, les laboratoires Merck, la compagnie de transport maritime Maersk, ou bien le groupe publicitaire WPP. L'Ukraine a tout de même été la principale victime (Banques, Aéroports, Transports en commun, etc.). En terme d'enjeux financiers, la demande de rançon s'élevait à 300 USD en Bitcoins (intraçable, assez classique pour les rançons d'attaques cyber), mais la récolte n'a été "que" de l'ordre de 10 000 USD. Après coup, on pourrait plutôt qualifier NotPetya de logiciel "*wiper*", qui détruit tout, parce que même les entreprises ayant payé n'ont pas récupéré l'intégralité de leurs données. Certaines compagnies ont été fortement touchées, comme par exemple Merck pour 900m USD (dont 300m USD en police cyber). Les polices perte d'exploitation (PE) et responsabilité civile (RC) également atteintes : En terme de PE la perte a été limitée car les couvertures ont des limites lorsqu'il n'y a pas de dommage à proprement parler. Il n'y avait pas (ou peu) d'exclusion pour le cyber, donc les polices "tous risques" furent affectées. A propos de la RC, l'exposition est souvent sous-limitée par le montant des dommages immatériels non consécutifs (DINC). Nous avons là un cas classique d'exposition cyber "silencieuse".

"Sony" : Au mois de Novembre 2014, la filiale Américaine du groupe Japonais Sony a été la cible d'une perturbation cyber de grande ampleur : C'est l'une des intrusion informatiques qui marquera le plus les professionnels de la distribution, tellement importante que les États-Unis ont soupçonné l'état de Corée du Nord d'en être instigateur [106]. En effet, l'intrusion est intervenue après la publication du film "*The Interview*" qui raconte un complot d'assassinat sur le dirigeant Nord-Coréen

102. Algorithme gratuit mis en ligne par Benjamin Delpy, voulant prouver à Microsoft que leur système de sécurité était vulnérable. L'application permet d'enregistrer des codes d'authentification en ligne
103. Source : *"2017 cyber attacks on Ukraine"*, Wikipedia 2019.
104. Les premières contaminations ont commencé 27 Juin 2017 à 11h
105. *Ransomware* apparu en Mars 2016, déjà connu des experts informatique.
106. 20 Minutes, 21 Décembre 2014

Kim Jong Un. L'attaque a consisté en une récupération de données sensibles dans les serveurs de *Sony Entertainment Pictures*, puis d'une tentative d'intimidation, et enfin d'une fuite sur internet de plusieurs films prévu en salle de cinéma pour les prochains mois [107]. Le groupe responsable du piratage signait ses actions par "#GOP" traduit par *"Guardian of Peace"*, soit "Gardien de la Paix". L'incident a été rendu possible par l'utilisation combinée d'un SMB [108] (*Server Message Block*) [109], ainsi qu'un ensemble d'outils permettant de pénétrer le serveurs, d'en extraire de l'information puis l'altérer, et cela de manière répétée indéfiniment [11]. Suite à cette affaire, l'entreprise Sony a réclamé à ses assureurs le remboursement d'une partie de ses pertes, notamment les sommes versées dans le cadre des obligations de notification des clients atteints au titre de son contrat de responsabilité civile [15]. La Cour Suprême Américaine de New York a finalement refusé la demande de Sony Corporation, en explicitant que ces frais n'étaient pas couverts par les contrats traditionnels (ni en dommage, ni en RC).

"Target" : La Target Corporation est l'une des plus grosses entreprises de grande distribution des États-Unis. Elle a été la cible fin 2013 d'une attaque cyber massive sur ses serveurs, résultant à la perte à large échelle de données clients. La chaîne de magasins a en effet révélé une perte d'environ 40 millions de numéros de cartes bancaires, ainsi que leur date d'expiration et les cryptogrammes au dos, de près de 70 millions de noms, adresses (mails et postales), numéros de téléphones de clients. Soit environ 110 millions de clients touchés [110]. Les conséquences ont été profondes pour l'entreprise, qui a annoncer sa vulnérabilité, faire face à plusieurs procès, assister à la chute de sa popularité et de son chiffre d'affaire (CA), et enfin voir Gregg Steinhafel (CEO) démissionner 5 mois après le vol. D'autres sinistres similaires ont vu le jour dans l'année suivante, et Target n'a pas été la seule victime de ce mode d'action [111].

"Snowden" : Edward Snowden est un citoyen Américain. Son nom est largement connu du grand public car il a été la source de divulgation d'informations hautement confidentielles concernant le gouvernement Américain, en 2013. Par l'intermédiaire des journaux *The Guardian* et *The Washington Post*, l'informaticien a rendu public plusieurs programme d'espionnage de la population [112]. Si on ne peut pas vraiment à proprement parler d'une attaque cyber (bien que la définition soit relativement ouverte) ni de piratage informatique, on peut corréler cette histoire avec les effets d'une intrusion ou d'une perte de données sensibles. En effet, les conséquences ont été désastreuse pour l'état Américain et s'en est suivi un scandale qui n'a toujours pas été étouffé, et qui continue d'effrayer les entreprises. Il est désormais résident sous asile politique en Russie. Son histoire a ins-

107. On peut citer notamment "Fury", *blockbuster* à $ 70m de budget, affichant Brad Pitt et Shia Labeouf au casting
108. Source : SecurityWeek, 2014.
109. Il s'agit d'un ver informatique permettant de diriger l'attaque
110. Source : Next Impact, 13 Janvier 2014.
111. La chaîne de boutique de luxe Neiman Marcus est attaquée en Janvier 2014 par un procédé similaire, même si d'ampleur moindre.
112. *PRISM*, *XKEYSCORE*, et *Boundless Informant* pour ne citer qu'eux. Source : Le Monde, Juin 2013

piré un film éponyme [113] à succès. en parallèle à Edward Snowden on pourrait citer Kevin Mitnick, l'un des plus célèbre cyber criminel, recherché notamment par le FBI pendant plusieurs années (auteur d'une traque avec les services de police et de plusieurs tentatives d'évasion). Il a été arrêté puis incarcéré (condamné à 5ans de prison ferme en 1995, à l'époque la plus lourde peine jamais infligée pour un délit informatique) avant d'être remis en liberté en 2000 et devenir une référence parmi les experts en sécurité cyber.

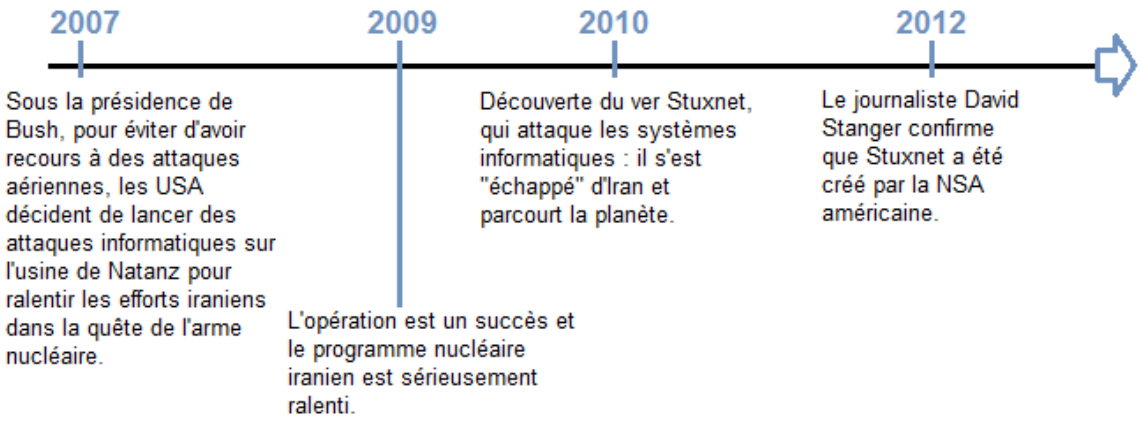
113. "Snowden" de Olivier Stone, sorti en 2016.

Annexe B : Explosion des centrifugeuses de Natanz, Iran [114]

Américains et Israëliens, espéraient depuis longtemps déranger les velléités militaires nucléaires de l'Iran. Les Iraniens avaient protégé leurs systèmes numériques nucléaires en les isolant géographiquement de tout réseau. Il était donc nécessaire d'accéder directement à un site, pour y implanter le virus qui pénétrerait les équipements. Pour les États-Unis, la NSA est à la manoeuvre, tandis que côté Israëlien, c'est l'unité 8200, spécialisée dans la guerre cyber est intégrée à l'opération. Les Américains disposaient de centrifugeuses similaires à celles des Iraniens, qui leur avaient été fournies fournies par le dictateur Lybien Mouammar Khadafi après qu'il eut renoncé à ses efforts nucléaires en 2003. Le virus sera introduit dans les systèmes iraniens à travers la mise à jour des ordinateurs portables des ingénieurs de l'usine de Natanz, moins surveillée que les installations elles-mêmes. Après la destruction de quelques centrifugeuses, les Iraniens blâmant la piêtre qualité des machines fournies par le Pakistan, bloquèrent les autres.

Côté américain, l'opération *Olympic Games*, dont Stuxnet est un élément, a été commandée par le général E. Cartwright et supervisée personnellement par le président G. W. Bush. Elle a rapidement fait l'objet d'une coopération étroite avec les Isrëliens, associés dans délai. Courant 2009, le programme fonctionne avec succès. Le projet nucléaire iranien est ralenti, sans que ses responsables aient soupçonné la source de leurs problèmes. En 2010, les premiers articles de presse sur un nouveau ver informatique nommé Stuxnet commencent à paraître. Le secret va dès lors, être éventé.

L'opération *Olympic Games* a fait partie d'un ensemble de mesures (assassinats ciblés, embargo, etc.) visant à affaiblir les efforts nucléaires de l'Iran. Il était nécessaire de rendre le pays plus conciliant dans la perspective d'un accord sur le nucléaire (finalement conclu le 14 juillet 2015 à Vienne, Autriche). Il s'est donc agit d'une opération politique. Cet édifice diplomatique a été jeté bas par le président Donald Trump, qui s'est retiré de l'accord avec l'Iran en 2018, initiant un nouveau bras de fer.



114. Source : "espions", exposition à la cité des sciences et de l'industrie (Paris, France), 2019-2020.

Annexe C : TV5 Monde [115]

Dans la nuit du 8 au 9 avril 2015, trois mois après les attentas de Charlie Hebdo et de l'Hyper Cacher, une attaque inédite est lancée contre TV5MONDE, chaîne francophone internationale, quelques heures après l'inauguration de leur nouvelle chaîne dédiée à l'art de vivre à la française. Les écrans des 11 chaînes du diffuseur s'éteignent dans le monde entier. En parallèle, les comptes Twitter et Facebook de la chaîne sont piratés, des messages de soutien à l'état islamique en anglais, arabe et français y sont publiés. Bien loin de la revendication initiale de l'attaque par des islamistes radicaux, me piratage est attribué à un groupe de pirates informatiques russes bien connus [116]. Les dégâts informatiques sont considérables. TV5MONDE a été près de disparaître pour plusieurs mois : son système d'exploitation, ses routeurs et l'ensemble de ses moyens étaient mal protégés, par des mots de passe trop faibles.

Les sources reprises par les médias et désignant la Russie sont le plus souvent des sociétés informatiques cherchant l'origine des attaques subies par leurs clients : Client Securit Trust (Microsoft), FireEye, etc. Classiquement, les services de renseignement laissent dire, sans parler ouvertement de leurs indices afin de ne pas dévoiler leurs méthodes d'enquête. La presse désigne le renseignement militaire russe, le GRU. Les preuves manquent pour désigner le donneur d'ordre politique, mais tous les indices accusent le Kremlin, qui a cependant toujours démenti tout rôle dans cette affaire.

La Russie est experte en destabilisation. En jouant des techniques de propagande et de désinformation, entre autres, elle conduit une "guerre hybride" contre ses adversaires. Elle pense défendre les intérêts russes en aidant ses amis politiques partout dans le monde, en jouant très habilement et impunément sur des atouts que lui offrent les réseaux sociaux. Mais aussi la violation de données. Elle héberge l'ingénieur américain Edward Snowden, auteur de fuite majeures concernant des dossiers de la NSA. Dans le cas de TV5MONDE, les auteurs de l'attaque cyber ont sans doute cherché à faire taire une voix francophone émettant depuis Paris, qui avait critiqué l'intervention russe en Ukraine et bloqué quelques mois plus tôt la vente de navires de guerre Mistral. Du point de vue de ses organisateurs, le succès de l'opération ne peut faire aucun doute.

115. Source : "espions", exposition à la cité des sciences et de l'industrie, 2019-2020.
116. Ils possèdent plusieurs pseudonymes dont APT28, Sednit, Sofacy, Pawn Storm, Fancy bear, Strontium, etc.

Annexe D : Éventail des méthodes de piratage informatique [117]

- **Malwares** : Un programme malveillant ("*malware*" ou "maliciel") désigne tout type de logiciel essayant d'infecter un objet connecté (ordinateur, téléphone mobile par exemple). Les attaquants se servent de maliciels pour extraire des informations ou des codes d'accès, détourner de l'argent ou bloquer l'utilisation de l'appareil. Des logiciels existent pour s'en protéger ;
- **Spying** : Un logiciel espion est un type de maliciel dont se servent les pirates pour espionner afin d'obtenir des données personnelles bancaires par exemple, ou des informations de connexion (sites visités, durée, etc.) ;
- **Adwares** : Un *adware* est un type de logiciel qui lance à répétition des fenêtres "pop-up" publicitaires, pouvant nuire au bon fonctionnement d'un ordinateur, et afficher de la publicité illégalement.
- **Hameçonnage** (*phishing*) : L'hameçonnage (appelé également "*phishing*") consiste à inviter la cible à révéler des informations sensibles par un *e-mail* ou un site internet factice, en se faisant passer pour quelqu'un de légitime ;
- **Virus** : Un virus informatique est un programme qui est introduit dans un appareil sans autorisation. Certains d'entre eux sont seulement nuisibles pour l'ordinateur, mais la plupart sont même pires : ils détruisent, abîment ou prennent contrôle de certaines fonctionnalités. Le virus à la particularité de pouvoir se répandre par les réseaux en se multipliant (comme en biologie) ;
- **Cheval de Troie** (*data pipeline*) : Comme dans l'Iliade, le cheval de Troie (ou "*Trojan horse*") est un outil qui d'apparence semble bienveillant mais cache en réalité un virus. Les "*Trojan*" sont souvent des pièces jointes interposées dans un téléchargement ou un *e-mail* ;
- **Worm** : Les vers informatiques (*worms*) sont des codes qui se répandent dans un réseau en se répliquant ;
- **Form Jacking** : Comme son nom l'indique, il s'agit du fait d'intercepter les informations lorsque l'individu rempli un formulaire sur un réseau, il s'agit le plus souvent de données bancaires, utilisées ensuite pour effectuer des paiements en ligne.
- **Rootkit** : Les pirates informatiques souhaitent obtenir un accès administrateur à l'appareil infecté pour mieux le contrôler. Pour réaliser cela en toute discrétion, ils utilisent un *rootkit*. Les *rootkits* ne peuvent pas se répandre seuls, mais sont souvent l'un des outils d'une attaque de plus large ampleur ;
- **Ransomware** [118] : Les logiciels de rançon fonctionnent comme une prise d'otage : Le logiciel force l'entrée et bloque l'accès à l'information (base de données, outils, ...). Il demande ensuite

117. Source : Avast, 2019.

118. Nous choisissons volontairement de laisser le mot anglais, que l'on retrouve plus largement que sa traduction "rançonlogiciel", même dans la littérature francophone.

le règlement monétaire (souvent en Bitcoin) pour s'extraire. Certaines des atteintes les plus célèbres (et destructrices) proviennent de *ransomwares* : WannaCry, Petya, ... Les *ransomwares* sont imaginés par des pirates habiles et sont souvent introduits dans un ordinateur par une pièce jointe ou par le réseau ;

- **Détournement de navigateur** : Un maliciel modifie les paramètres de l'explorateur de l'ordinateur et envoie l'utilisateur sur des pages internet qu'il n'avait pas l'intention de visiter ;
- **Enregistreur de frappe** : Les enregistreurs de frappe, comme leur nom l'indique, sont des logiciels s'en prennent au clavier relié à l'ordinateur infecté, en enregistrant ce qui est écrit (mots de passe, numéro d'identification bancaire, etc.) ;
- **Hacker** : Le piratage informatique représente la manipulation d'un ordinateur et des systèmes qui lui sont connectés. Il est généralement effectué en utilisant des scripts ou des programmes qui manipulent les données en passant pas une connexion réseau afin d'accéder aux informations du système. Les techniques de piratage incluent virus, chevaux de Troie, rançongiciels, détournements de navigateur, rootkits et attaques par déni de service.
- **Scam** : Il existe de nombreux scams en ligne mais ils ont tous un point en commun : ils vous incitent tous à révéler vos informations personnelles ou à payer quelque chose que vous ne recevrez jamais. Les types de scams les plus répandus sont des scams par *e-mail* comme les arnaques à la nigériane, les arnaques aux sentiments, les arnaques sur les sites de petites annonces etc.
- **Ingénierie sociale** : L'ingénierie sociale exploite la crédulité de l'utilisateur. Ce dernier est poussé à livrer ses données personnelles, et donc se faire pirater. Par la menace ou la tentation, l'arnaque incite à livrer des informations confidentielles ;
- **Usurpation d'identité** : Elle peut présenter deux issues :
  - Les informations personnelles sont utilisées pour créer de nouveaux comptes ;
  - Les informations personnelles sont utilisées pour se connecter aux comptes existants.

  Dans les deux cas, le but final est d'effectuer des achats ou des retraits financiers en votre nom ;
- **Botnet** : Un *botnet*, c'est-à-dire un ensemble de (ro)bots, est un réseau composé d'un grand nombre d'ordinateurs qu'un maliciel contrôle. Ainsi toute action ordonnée par le pirate sera effectuée multipliée par 1 000, 10 000 (le nombre de machines infectées) et donc entraînera des conséquences dévastatrices ;
- **Sniffing** : Un renifleur n'est pas nécessairement malveillant. Il est créé pour espionner et enregistrer les actions d'une machine connectée. Il peut notamment être utile pour détecter une anomalie ou un défaut de fonctionnement. Il est très difficile à détecter ;
- **Distributed Denial-of-Service attack** (Mass DDoS) : L'attaque de masse, coordonnée, qui a pour but de mettre hors service le site internet de l'entreprise visée, entraînant ainsi non

seulement une perte d'exploitation, mais également un défaut d'image, de crédibilité auprès du public. Le *Mass DDoS* est en quelque sorte l'inondation du réseau par une demande de très (trop) grande ampleur. Ainsi, bloquer la source ne permet pas d'interrompre le processus de perturbation étant donné qu'elle provient de multiples périphériques ;

- **Cloud Provider Failure / Cloud Compromise** : La panne de *cloud* : Cette attaque vient rompre la liaison entre l'activité de l'entreprise et son *cloud* : ainsi les opérations sont interrompues par défaut de services habituellement possibles grâce au *cloud.* Le ***cloud computing*** est une technique d'enregistrement et de stockage de l'information par serveurs externalisés ;
- **Financial transaction interference / Financial Theft** : Interruption d'un procédé de paiements (malversements). Cette menace peut avoir lieu de différentes façons : sur un site de paiement en ligne, par une fraude volontaire (arnaque), par un vol de coordonnées bancaires ;
- **Cyber Extortion** : Il s'agit de l'attaque utilisant un rançon-logiciel (ransomware), dont le principe est le suivant : le cybercriminels s'introduit sur un réseau et prend en otage des fichiers nécessaires au bon fonctionnement de l'entreprise (données comptables par exemple) et exige qu'une rançon soit payée pour libérer les données cryptée. L'écran d'ordinateur ciblé affiche alors le déroulement de l'agression et la demande de rançon sous menace de supprimer définitivement les fichiers. L'intrusion initiale se fait souvent à l'aide d'*e-mails* **"phishing"** (hameçonnage). Les cibles de ce type de perturbation sont plutôt les moyennes entreprises du fait des standards de sécurités trop élevés et donc infranchissables des grandes firmes ;
- **Wiper** : Le *wiper* est un logiciel implémenté par des pirates informatiques malveillant, qui est introduit dans une machine et détruit tout ce qu'il peut. Comme son nom l'indique, son unique but est d'endommager l'ordinateur hôte. Il entre en jeu souvent après une atteinte pour sortir sans laisser de trace.

Annexe E : Éventail des méthodes de piratage informatique (dommage aux biens)

- **Property Fire** : Le "*Property Fire*" est un type d'attaque cyber physique qui exploite différentes vulnérabilités des machines connectées et leurs microprogramme de gestion des engins. Cela crée une surconsommation et entraîne une surcharge thermique dite "fugitive" ;
- **Industrial Facilities** : Les agressions sur des installations industrielles sont fréquentes, elles utilisent des accès sous les contrôles automatiques par les logiciels et négligent les alertes afin de provoquer des incendies industriels ou explosions ;
- **Spoofing** : Envoyer de fausses informations aux capteurs/récepteurs ;
- **Hysteresis** : Il s'agit de la propriété d'un système dont l'évolution ne suit pas le même comportement selon qu'une cause extérieure augmente ou diminue ; [119]. L'hystérésis est une forme d'attaque informatique qui referme une boucle et force ainsi un appareil connecté à travailler en cycle. Ces cycles s'accélère et finissent par détruire l'outil ;
- **Disconnection** : Pénétrer un réseau fermé et procéder à la déconnexion d'un système, ce qui résulte à éteindre une fonctionnalité d'un appareil ;
- **Actuators** : contrôler des composants physiques (par exemple un bras articulé dans une usine), des robots connectés.

119. Hystérésis, Wikipedia 2019.

Annexe F : *Cyber hygiene*, solutions de protection des machines connectées

- **Le "firewall"** : Traduction littérale du pare-feu ou mur de feu, le *firewall* est un système informatique, un logiciel permettant de sécuriser un réseau. Le principe est qu'il bloque l'accès pour les tentatives de connexions externes n'étant pas répertoriées comme sûres : Pour chaque entrée, il associe une règle de gestion et une action. Le *firewall* traite ainsi les entrées dans le réseaux. Il se présente la plupart du temps comme un simple boîtier, qui peut être directement intégré à l'ordinateur concerné. Attention, le pare-feu n'est pas une arme de défense absolue, certaines intrusions dites "cheval de Troie" peuvent être camouflée et créer des brèches pour laisser des attaques pénétrer le système ;
- **Le "honeypot"** : Comme son nom l'indique, il s'agit d'une sorte de proie pour attirer les tentatives d'intrusion vers des ressources et ainsi les identifier et les détruire. C'est une méthode de défense cyber usuelle : on fait croire à l'attaquant qu'il peut prendre le contrôle de l'ordinateur, et pendant qu'il s'exerce, on peut préparer une réponse adaptée à sa composition. Il fonctionne en deux phases : la surveillance des ressources et la compréhension de l'information ;
- **Le chiffrement des données** est une sorte d'anti-vol : de nombreux logiciels simples d'utilisation permettent cela : avec la multiplication des échanges et la démocratisation de l'*e-mail*, chiffrer ses données est la moindre des protections. Le chiffrement consiste à transformer le contenu de l'information, en donnant une clé de décodage à son interlocuteur. On peut également chiffrer un PC (*personal computer*), un support d'information (de type clé USB par exemple), ou même ses recherches sur internet ;
- **La réplication** : En informatique, répliquer ses données consiste à multiplier les jeux de données sur plusieurs registres. Ainsi, avec un croisement des sources, on peut s'assurer de la véracité de l'information et de l'intégrité des logiciels utilisés en vérifiant simplement la cohérence de l'exercice. Cette méthode n'est pas une sauvegarde a proprement parler puisque les données sont toujours reliées et évoluent lorsque la source évolue, mais permettent de contourner les risques de panne ou d'intrusion cyber ;
- **La duplication** : Il s'agit du très simple *"Copy and paste"*. Comme son nom l'indique le principe de la duplication est de copier puis coller ses données ailleurs (sur un autre support) afin de posséder plusieurs sets d'informations et donc se protéger d'une perte totale en cas d'attaque ou de panne informatique ;

Annexe G : Précisions sur la régulation du cyber

Les Normes ISO 27000

L'ISO (Organisation internationale de normalisation)[120] est une filiale du conseil économique et social des Nations Unies qui a pour rôle d'établir et de recenser des normes dans divers secteurs d'activité. Dans le cas de la menace cyber nous nous intéressons aux normes 27000-27999 concernant la sécurité de l'information. Notons particulièrement que seule la norme ISO 27001 soumet les exigences en terme de gestion de la sécurité des informations (SMSI[121]). Elle permet de certifier des organisations. La norme est structurée de la façon suivante[122] :

- Phase "*Plan*" : établissement : on détermine ici les objectifs du SMSI
  - étape 1 : politique et périmètre du SMSI ;
  - étape 2 : identifier le risque, élaborer le plan de sécurité ;
  - étape 3 : traiter la menace et identifier les risques résiduels ;
  - étape 4 : choisir les mesures de sécurités adaptées à mettre en place.
- Phase "*Do*" : implémentation : c'est la procédure de mise en route pour atteindre les objectifs fixés précédemment. Établissement du plan, déploiement des mesures de sécurité et sensibiliser le personnel ;
- Phase "*Check*" : maintien (gestion courante de la politique) ;
- Phase "*Act*" : amélioration et pilotage des mesures.

Le norme ISO 27002 est une aide à la préparation pour la norme précédente et offre une sorte de guide de référence pour y parvenir. Les normes ISO jouent un rôle important dans la gestion du risque cyber, car ce dernier menace particulièrement les détenteurs de bases de données personnelles (comme les informations médicales ou bancaires par exemple).

Le règlement RGPD

Le RGPD (ou GDPR[123] en anglais) est le règlement général sur la protection des données. Il concerne les membres de l'Union Européenne (UE) et a pour vocation de protéger les individus et leurs données personnelles, en explicitant des règles et en harmonisant celles-ci à l'échelle de l'UE. Promulgué en 2016, il est officiellement entré en vigueur en 2018. On lui doit notamment l'apparition des notifications *cookie* lorsque l'on navigue en ligne[124].

120. Voir annexe H : "Normes ISO 27".
121. La norme ISO 27001 définit les règles à suivre afin de mettre en place un SMSI : système de management de la sécurité de l'information
122. ISO/CEI 27001, Wikipedia 2019
123. General Data Protection Regulation
124. Un *cookie* est un petit fichier informatique, un traceur, déposé et lu par exemple lors de la consultation d'un site internet, de la lecture d'un courrier électronique, de l'installation ou de l'emploi d'un logiciel ou d'une application mobile et ce, quel que soit le type de terminal utilisé. L'utilisation de ces outils est soumise à votre consentement dès lors qu'ils ne sont pas strictement nécessaires au fonctionnement du site concerné. (Source : CNIL.fr, 2019)

La norme PCI DSS

La conformité à la norme PCI DSS (Payment Card Industry Data Security Standard) est très importante dans le cadre de la gestion des paiements par carte bancaire. Afin d'augmenter la sécurité de la transaction monétaire, les principaux réseaux de cartes de paiement (c'est-à-dire Visa ®, MasterCard ®, American Express ®...) ont mis en place un système de contrôle avancé des utilisations de ces cartes et des TPE (terminal pour encaissement) avec l'intention de réduire les fraudes. Ces recommandations s'appliquent pour les CDE [125] : environnement informatique possédant des informations de carte de crédit lors d'un paiement.

La directive sur les services de paiement

La directive sur les services de paiements (DSP) est une directive européenne de 2007 qui concerne les transactions dans le marché intérieur. La DSP 2 vient compléter cette dernière en 2018, rendant notamment obligatoire l'authentification forte [126] lorsque le montant dépasse 30 EUR pour les paiements en ligne. La DSP 2 vient également interdire la sur-facturation lors du paiement parte carte bancaire et renforce les droits des consommateurs (abaissement de la franchise en cas de fraude). En septembre 2019, de nouvelles dispositions concernant à l'accès à ces données seront mises en place : il s'agit des standards techniques réglementaires.

La directive NIS

La directive *Network and Information Security* s'inscrit dans la stratégie de l'UE en matière de sécurité cyber. Adoptée en 2016, il s'agit de l'une des premières réglementations européennes concernant la menace cyber. Cette directive est décomposable en trois parties :

- Augmenter les capacités nationales des états membres de l'UE à combattre la cyber criminalité ;
- Améliorer la collaboration des pays voisins entre eux dans cette lutte ;
- Harmoniser la supervision étatique des secteurs d'activité risqués.

Après son entrée en vigueur en janvier 2018, les membres de l'Union Européenne ont dû s'aligner au niveau national sur cette directive avant le 9 mai 2018. Cette directive sera suivie en 2019 par les RTS (normes techniques réglementaires). La France avait déjà fait appliquer des conditions similaires à certaines entreprises, les "organismes d'importance vitale" (OIV), par la loi française de programmation militaire (LPM) [127].

Quelques précisions sur les régulateurs à présent. Nous avons présenté dans les grandes lignes les différents acteurs dans le corps principal du mémoire, voici un complément.

125. *cardholder data environment*
126. Au moins 2 facteurs parmi les suivants : mot de passe (ou code), confirmation mobile sur un autre appareil, empreinte digitale, voix, iris, ...
127. L'article 22 de la LPM (2013), impose le renforcement de la sécurité des réseaux et systèmes d'information des OIV. Source : ANSSI, 2019.

ENISA

L'Agence européenne chargée de la sécurité des réseaux et de l'information [128] (ou bien "*European Union Agency for Cybersecurity*", créée en 2004 -et active depuis 2005-), propose des recommandations sur la gestion du risque informatique et intervient dans la mise en oeuvre de politique de sécurité des systèmes numériques. En plus de proposer un cadre réglementaire, l'ENISA est chargée de sensibiliser les individus et les professionnels à ce risque, et de proposer des exercices de prévoyance. L'ENISA est notamment à l'origine de la directive NIS avec la commission européenne. Le "*EU Cybersecurity Act*" (paru le 7 Juin 2019) présente une structure permanente européenne, pour informer du cyber entre les pays membres de l'UE et proposer des solutions d'entraide. Cette loi offre de renforcer les moyens de l'UE en terme de sécurité informatique afin de lutter contre le risque cyber et propose une certification en matière de sécurité cyber (avec 3 niveaux de certificats). C'est pourquoi une plateforme de certification impartiale et normalisée, soutenue par des laboratoires accrédités, est nécessaire pour permettre aux fabricants d'appareils et aux fournisseurs de services de vérifier la sécurité des appareils, ainsi que de classer et sélectionner le type de protection le plus approprié pour leur produit [129].

CNIL

La CNIL (Commission nationale de l'informatique et des libertés) est une autorité administrative française. Indépendante du gouvernement, la CNIL veille à la protection des droits des individus dans l'utilisation de l'informatique pour le traitement des données personnelles. Depuis que ces règles de conformité pour la protection de l'intégrité des données et le RGPD ont été mis en place, la CNIL en assure l'application.

ANSSI

L'ANSSI (Agence nationale de la sécurité des systèmes d'information) relève de la SGDSN (Secrétaire général de la défense et de la sécurité nationale) et est chargé de la sécurité informatique au niveau national. L'ANSSI à notamment publié un guide d'hygiène informatique en 2017 et mis en ligne un MOOC [130] ("secnumacademy") de formation à la cyber sécurité. L'ANSSI est l'organe à contacter en cas d'incident "affectant la sécurité ou le fonctionnement des systèmes d'information d'importance vitale (SIIV)".

CEPD

Le CEPD (Contrôleur Européen de la protection des données), ou EDPS en anglais, est créé en 2004 avec l'ambition de contrôler les institutions d'Europe et leurs utilisations des données (particulièrement les données personnelles et la vérification que le droit à la vie privée est respecté). Il s'agit d'un contrôleur indépendant de l'Union Européenne.

128. Anciennement "*European Network and Information Security Agency*", d'où son acronyme ENISA.
129. Source : *IoT Business News*, 2019.
130. Massive Open Online Course : type de formation à distance en ligne

ACPR

L'ACPR (autorité de contrôle prudentiel et de régulation) se charge de la supervision des assurances, mutuelles et banques au niveau national. Depuis 2018, l'ACPR a affirmé vouloir s'occuper du risque cyber plus en profondeur en offrant un cadre précis, et a publié un "document de réflexion". Une consultation a revue ce texte en 2018 [131] :

131. Source : assurlandpro.com, 2018

Annexe H : Normes ISO 27 [132]

Normes ISO 27	
ISO/CEI 27000	Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire (2018)
ISO/CEI 27001	Système de Gestion de la Sécurité de l'Information (ISMS) — Exigences
ISO/CEI 27002	Code de bonnes pratiques pour la gestion de la sécurité de l'information (anciennement ISO/CEI 17799)
ISO/CEI 27003	Système de Gestion de la Sécurité de l'Information (ISMS) — Guide d'implémentation
ISO/CEI 27004	Mesure de la sécurité de l'information
ISO/CEI 27005	Gestion du risque en sécurité de l'information
ISO/CEI 27006	Exigences pour les organismes réalisant l'audit et la certification de Systèmes de Gestion de la Sécurité de l'Information (ISMS)
ISO/CEI 27007	Guide pour l'audit de Systèmes de Gestion de la Sécurité de l'Information (ISMS),en préparation
ISO/CEI 27008	Lignes directrices de vérification en matière de mesures de sécurité,en préparation
ISO/CEI 27011	Guide pour l'implémentation de ISO/CEI 27002 dans l'industrie des télécommunications (publié le 15 décembre 2008)
ISO/CEI 27013	Guide sur la mise en œuvre intégrée de l'ISO/CEI 27001et de l'ISO/CEI 20000-1
ISO/CEI 27017	Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/CEI 27002 pour les services du nuage(autre nom UIT-T X.1631, révision courante 2015)4
ISO/CEI 27018	Code de bonnes pratiques pour la protection des informations personnelles identifiables(PII) dans l'informatique en nuage public agissant comme processeur de PII
ISO/CEI 27031	Code de bonnes pratiques en matière de Technologies de l'information – Techniques de sécurité – Lignes directrices pour mise en état des technologies de la communication et de l'information pour continuité des affaires (publié le 1er décembre 2012)
ISO/IEC 27032	Technologies de l'information - Techniques de sécurité - Lignes directrices pour la cybersécurité
ISO/CEI 27034	Sécurité des applications
ISO/CEI 27035	Gestion des incidents
ISO/CEI 27036	Sécurité d'information pour la relation avec le fournisseur
ISO/CEI 27037	Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques (publié le 15 octobre 2012)
ISO/CEI 27038	Spécifications pour la rédaction numérique
ISO/CEI 27039	Sélection, déploiement et opérations des systèmes de détection d'intrusion (publié le 11 février 2015)
ISO/CEI 27799	Informatique de santé - Gestion de la sécurité de l'information relative à la santé en utilisant l'ISO/CEI 27002

132. Source : "Liste des normes ISO", Wikipedia 2019

Annexe I : Précisions sur le marché d'assurance cyber en France

En ce qui concerne les offres du marché assurantiel français, le tableau ci-dessous nous présente un récapitulatif de ce que contient une garantie cyber :

Gestion de crise	Dommages (1st party)	RC (3rd party)
Mesure d'urgence	Nettoyage des données et logiciels	RC transmission de virus
24/7 hotline	Restauration des données	RC Vie privée
Coût d'investigation informatique	Extorsion (paiement de la rançon)	Déni de service sur tiers
Coût d'assistance juridique	Perte d'exploitation	
Restauration		
Coût de gestion de crise		
Communication de crise		
Mise en conformité sur la protection des données		

Table 41 – La composition d'une assurance cyber

Enfin, l'état général du marché assurantiel français est résumé dans le tableau à double entrée ci-après qui nous permet d'avoir une bonne vue d'ensemble sur les offres disponibles. On peut donc observer les particularités des contrats offerts en fonction du type de client auxquels la compagnie d'assurance s'adresse.

PRODUITS	PARTICULIERS	DÉDIÉS AUX PROFESSIONNELS	SUR MESURE PME	ENTREPRISES
Clients Cibles	Particuliers Extension MRH par ex Protection juridique	Professionnels TPE & PME/PMI CA < 1M	Professionnels TPE & PME/PMI CA > 1M	Entreprises dont le CA est important
Garanties types	E-réputation, usurpation d'identité, utilisation frauduleuse de moyens de paiement et protection juridique	Atteinte au SI et aux données, Cyber extorsion, PE, RC, Volet service	Atteinte au SI et aux données, Cyber extorsion, PE, RC, Volet service	Sur mesure
Limites types	10 000 € dont 5 000€ pour l'indemnitaire	150 000 € - 500 000 €	500 000 € - 10 000 000 €	Sur mesure jusqu'à 300 – 400 M€ de capacité
Vente	Systématiquement en inclusion	Majoritairement par extension	Extension ou police spécifique	Police spécifique
Primes	Quelques euros	Fonction du CA et des garanties, 250 € - 1 000 €	Fonction du CA, du secteur, du nombre d'employés	Fonction du CA, Secteur nombre d'employés

Table 42 – Segmentation des offres du marché français

Annexe J : Le marché des particuliers

Aux États-Unis

Il s'agit aux États-Unis d'un marché d'ores et déjà bien développé au travers notamment de polices spécifiques (*Stand alone*), d'extension à certaines polices (particulièrement en multirisque habitation pour les maisons connectés par exemple), ou encore avec les extensions fournies par des institutions financières (carte bancaire, paiements en ligne, etc.). Les caractéristiques de ces polices en Amérique sont les suivantes :

- Limites : [25 000 - 250 000] EUR ;
- Franchises : [0 - 1 000] EUR ;
- Primes : de quelques dizaines de dollars jusqu'à 1 600- 2 000 USD ;
- Services additionnels : Prévention, réponse post-incident, cellule de gestion de crise.

Les garanties que l'on retrouve le plus dans les polices destinées aux particuliers sont la menace d'extorsion (prise en charge des dépenses et rançons nécessaires pour mettre fin à une menace de divulgation de données personnelles sensibles), la fraude (frais et pertes consécutives à fraude à la carte de crédit, transfert d'argent par voie électronique), harcèlement cyber , protection de l'activité professionnelle, etc.

En 2018, 352 000 plaintes ont été déposées par des particuliers pour des crimes cyber (aux États-Unis), pour un préjudice total de 2,7 milliards de dollars (donc une moyenne de 7 670 USD par plainte).

En France

En France, le marché est bien moins développé que son équivalent américain : les polices sont souvent en inclusion ou en option dans des contrats. Les garanties en question sont souvent très limitées (franchises hautes ou/et limites courtes). En effet, les produits sont très basiques, parce qu'il existe très peu d'offre et très peu d'acteur sur le marché français. Les caractéristiques des polices disponibles sont les suivantes :

- Limites : [5 000 — 10 000] EUR ;
- Primes : quelques euros (souvent incluses dans une prime tierce -MRH, RC, ...-) ;
- Services additionnels : (parfois) un peu de prévention, un peu de réponse post-incident.

Les garanties que l'on retrouve le plus dans les polices destinées aux particuliers français sont l'usurpation d'identité (accompagnement d'un litige éventuel), atteinte à l'e-réputation (nettoyage, enfouissement et accompagnement dans les procédures de plainte), fraude aux moyens de paiements principalement.

Le marché français est support d'un fort potentiel de développement, mais le peu d'acteur et le manque de sensibilisation rend réticents les professionnels à (s')investir dans ce domaine.

Annexe K : Couvertures cyber

	Coverages
(1)	Breach of privacy event
(2)	Data and software loss
(3)	Network service failure liabilities
(4)	Business Interruption
(5)	Contingent Business Interruption
(6)	Incident response costs
(7)	Regulatory and defence coverage
(8)	Product and Operations Liability
(9)	Liability (Technology Errors & Omissions)
(10)	Liability (Professional Services Errors & Omissions)
(11)	Liability (Directors & Officers)
(12)	Multi-media liabilities (defamation and disparagement)
(13)	Financial theft & fraud
(14)	Reputational damage
(15)	Cyber extortion
(16)	Intellectual property (IP) theft
(17)	Environmental damage
(18)	Physical asset damage - Combined
(18.1)	Physical asset damage - Buildings
(18.2)	Physical asset damage - Contents
(19)	Liability (Death and bodily injury)
(20.1)	Operators Extra Expense
(20.2)	Control Of Well
(20.3)	Making Wells Safe
(20.4)	Cost Of Redrill
(20.5)	Physical asset damage - Oil Rigs
(20.6)	Structure
(20.7)	Equipment
(20.8)	Hull & Machinery
(20.9)	Increased Cost of Replacement
(20.10)	Pipelines
(20.11)	Removal Of Debris
(20.12)	Removal of Wreck
(20.13)	Oil Pollution Act
(20.14)	Offshore Pollution Liability Agreement
(20.15)	Seepage & Pollution
(20.16)	Sue & Labour
(20.17)	Total Loss Only

Annexe L : Analyse statistique de la base SAS : risque opérationnel

Cette base est constituée par SAS et recense des pertes opérationnelles. Cette dernière répertorie tout incident de montant supérieur à 1 000 000 USD, entre Mars 1971 et Juillet 2019. Ainsi, sont documentés plus de 35 000 événements dans tous les secteurs d'activité avec leurs caractéristiques. Notons que l'on entend ici comme risque opérationnel, toutes les incertitudes et les dangers auxquels une entreprise fait face lorsqu'elle exerce ses activités quotidiennes dans un secteur donné. Il s'agit d'un type de risque d'entreprise, il peut résulter de défaillances des procédures internes, des personnes et des systèmes, par opposition aux problèmes causés par des forces externes, tels que des événements politiques ou économiques, ou inhérents à l'ensemble du marché ou du segment de marché, appelés risque systématique.

Présentation de la base de données

Cette base de données est la propriété de SAS Enterprise, qui nous laisse l'étudier dans un objectif académique de recherche. Il s'agit d'une base de 35 967 évènements, avec 49 différentes colonnes, que l'on pourrait regrouper en 13 différents groupes. D'une part les informations sur les évènements, et d'autre part certaines précisions sur la bases. Intéressons-nous aux incidents reportés avec les 9 groupes de colonnes de la base :

- *"Key Descriptive Information"* : informations sur l'incident : numéro d'identification, nom de l'entreprise et de la firme atteinte ;
- *"Monetary Breakdown"* : Perte monétaire en million : description de l'évènement, montant des pertes brutes (en million de dollars US), le montant ajusté des CPI (IPC [133]). Nous pouvons noter que les évènements et les montants de pertes sont ajustés dans toute la base de données par monnaie et par indice de consommation ce qui les rends donc comparables ;
- *"Business Line Detail"* : Détail de l'activité en question : Code d'identification du groupe conforme à la norme de classification des événements et des effets de Bâle II (plusieurs niveaux de précision), libellés de ces niveaux. Une analyse à un niveau précis est donc rendue possible ;
- *"Event Risk Category Detail"* : Détail de l'évènement en question : idem que précédemment, code d'identification de l'évènement de perte (plusieurs niveaux de précision), libellés de ces niveaux ;
- *"Location"* : Détails géographiques, par pays et par siège social. Dans le cas du risque cyber, le pays où se situe le siège social à des conséquences sur la fréquence et le montant des pertes. On peut relever également le fait que les incidents de la bases proviennent du monde entier ;
- *"Key Dates"* : Informations temporelles sur la perte : début et fin du défaut, année de découverte de l'erreur. La temporalité est très importante pour estimer le coût d'un incident

133. Indice des prix à la consommation

informatique, parce que le fait de le prendre en compte rapidement permet de limiter les dégâts ;

- *"Industry Type/Region Information"* : Classification du secteur d'activité, autres données géographiques plus précises (régions) ;
- *"Firm Size Detail"* : Détail sur la taille de l'entreprise concernée : Chiffre d'affaire, nombre d'employés, résultat net, valeur de l'entreprise, etc.. ;
- *"Loss Effects Breakdown"* : décomposition des effets de perte : pertes légales, coût des actions de réponse, coût de la perte sur les actifs, coût de la réparation, etc. Ici on a également certains indices qui permettent d'imaginer s'il y a eu perte indirecte ou non et son ampleur.

Les précisions sur la base nous indiquent les dates de mises à jour de cette dernière, ainsi que les sources, les commentaires et autres glossaires et taux de change.

Description de l'algorithme de classification des incidents

Il a fallu ensuite séparer les incidents cyber des pertes opérationnelles non liées à un défaut de réseau ou une attaque informatique : cyber vs non-cyber. Nous avons pour cela utilisé une méthode de classification par recherche de mot clé. Nous disposons d'une description complétée soigneusement (taux de remplissage : 100%) qui explique l'évènement de perte dans la colonne *"Description of Event"*. Nous avions au préalable décrit dans les parties précédentes [134] plusieurs catégories et sous-catégories de risque cyber. Nous allons à présent nous aider de ces descriptions pour sélectionner un éventail de mots clés [3] nous permettant de classer les incidents de notre base [135]. Ces mots clés permettent d'identifier trois points essentiels pour définir une perturbation cyber, et donc un sinistre informatique entrant dans nos critères :

- Un **acteur** (*Actor*) : Nous avons une liste de 69 mots qui permettent d'identifier un acteur potentiel pour une intrusion informatique non-désirée. Nous avons pu séparer ces acteurs en 4 sous-catégories distinctes : Les actions humaines, les défaillances techniques du système, l'erreur du processus interne et enfin l'intervention d'un évènement extérieur ;
- Une **perte critique** (*Critical Asset*) : Liste de 39 mots pour une perte potentielle, qui désignent des cibles ou des actifs endommagés qui seraient susceptibles d'être révélateur d'une intrusion cyber ;
- Un **résultat** (*Outcome*) : 42 mots pour définir le type de sinistre, les dégâts qui résultent de l'incident et ainsi le classer ou non dans une perte cyber.

Ainsi avec un code de recherche par mot clé, nous avons identifié les incidents qui regroupent les trois caractéristiques (un acteur, une perte et un résultat) simultanément et sont donc, d'après notre hypothèse principale, issus d'une faille informatique et donc classés comme des perte cyber.

134. voir tableau 1 page 16.

135. Dans un soucis de continuité avec les travaux de Biener, Eling et Wirfs, nous avons repris la même liste de mots (voir Annexe M)

Nous pouvons ainsi effectuer quelques statistiques descriptives afin de pouvoir comparer la nature de nos risques, mais également les types de pertes, les montants, les zones géographiques ou encore les secteurs d'activité les plus touchés par la cyber sinistralité.

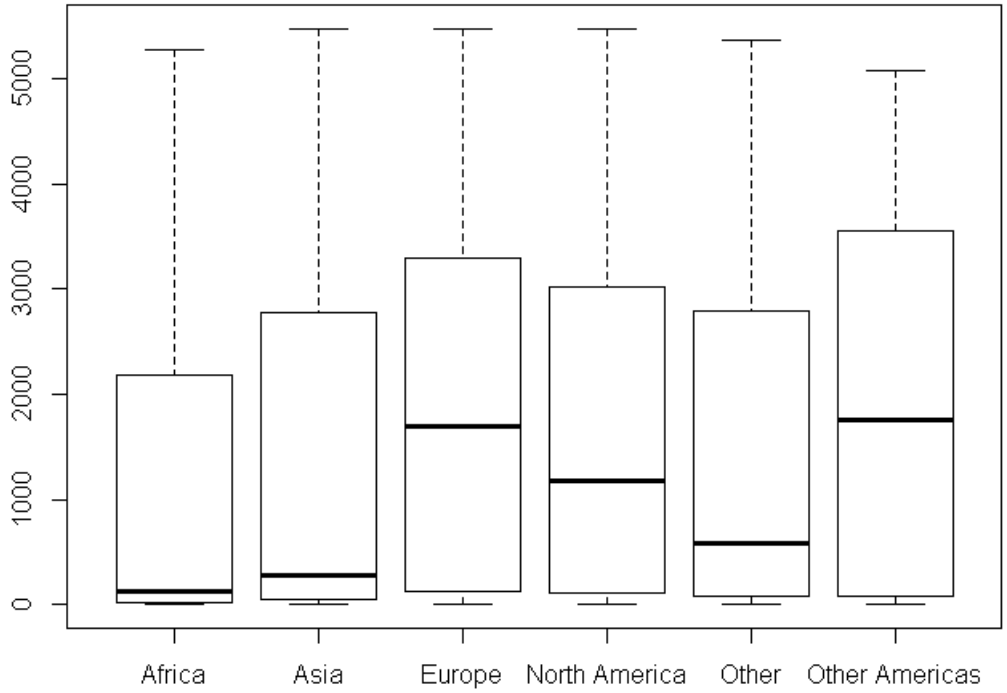


FIGURE 37 – *Boxplot* des montants par incident cyber par continent (million de USD)

En ce qui concerne la disparité par région pour les pertes opérationnelles cyber, la figure précédente nous montre des *boxplots* par continent. Nous pouvons donc facilement comparer à l'oeil les caractéristiques de ces incidents. Nous observons une grande disparité des maximums, minimums et médianes dans la base de données.

Le tableau ci-dessous résume une grande partie des informations qui nous intéresse dans la base de données. On peut y voir surtout un bon moyen de comparaison entre les pertes cyber et les pertes non-cyber. En effet, le panel A nous offre une série d'indicateurs mathématiques de bases qui permettent la mise en relief des différences caractéristiques entre risque informatique et les autres incidents opérationnels. Nous nous appuierons sur ce tableau pour étudier plusieurs des critères d'assurabilité.

Catégories	N	Moy.	Ecart-type	Min.	Q. 25%	Q. 50%	Q. 75%	Max.
Panel A : Cyber versus risque non-cyber								
Risque cyber	7 028	1 662,9	1 725,9	1,0	92,0	1 105	3 004	5 478
Risque non-cyber	28 939	1 853,9	1 717,9	1,0	146	1759	3365	5 483
Panel B : Sous-catégories du risque cyber								
Actions humaines	5 699	1 584,0	1 709,5	1,0	80	860	2 830	5 478
Défaillance technique du système	784	1 958,6	1 753,3	1,0	162,5	1 781	3 454	5 447
Erreur du processus interne	25	1 013,0	1 334,9	2,0	21	178	1 856	4 437
Evènement externe	520	2 113,0	1 760,7	1,0	216	1 896	3 499	5 447

TABLE 43 – Montant des pertes par risque (en millions US$)

Nous pouvons à présent illustrer ces chiffres avec quelques graphiques, dans le but d'une meilleure compréhension du contenu de cette base de données. Nous présentons ci-dessous un diagramme par secteur montrant la part des incidents cyber par rapport au risque opérationnel global représenté dans la base. Le risque que nous avons identifié comme technologique équivaut à une part de $\frac{7028}{28939} = 24\%$ de la base en nombre de lignes et $\frac{7028 \times 1662,9}{28939 \times 1853,9} = 22\%$ en terme de coût (montant des pertes).

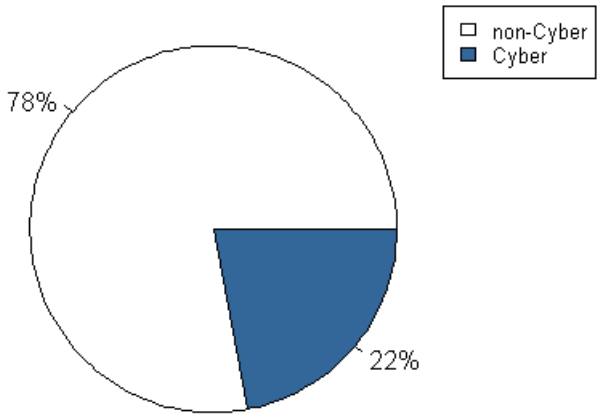


FIGURE 38 – Répartition des sinistres cyber (en montant des pertes)

Le diagramme en secteur ci-dessous représente le panel B du premier tableau. Il permet d'observer, parmi les incidents classés comme "cyber", la part de chaque cause. Rappelons que les quatre causes identifiées sont l'action humaine (qui est responsable d'après la base de 81,1% des pertes), la défaillance technique du système (11,1%), une erreur lors du processus interne (0,4%) et enfin un évènement externe (7,4%).

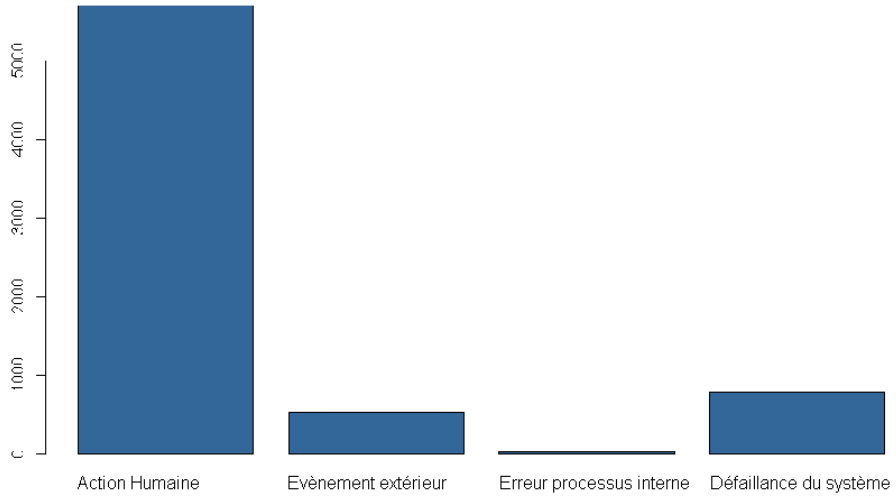


FIGURE 39 – Répartition des causes d'incident cyber

Nous concluons donc que pour le risque opérationnel, l'observation est la même que dans le risque cyber en général, ou de nombreuses études montrent que les causes humaines sont à l'origine de la majorité des incidents.

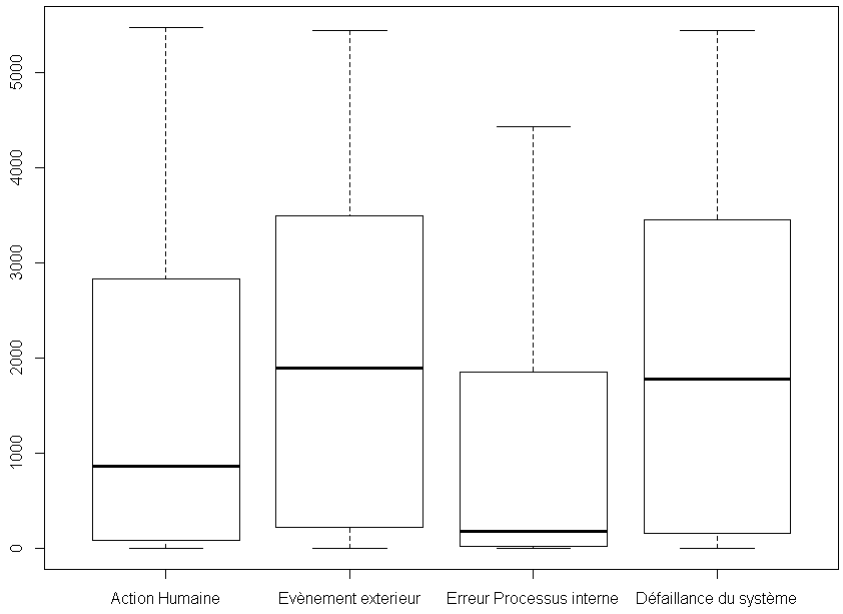


FIGURE 40 – *Boxplot* des montants de sinistre Cyber par acteur

Enfin, le dernier graphique que nous présentons dans ces statistiques descriptives de présentation de la base SAS OpRisk Global Data est un *boxplot* des montants de sinistre (en millions de USD) en fonction du type de source. Nous pouvons observer une fois de plus la grande hétérogénéité des résultats. Nous pouvons également tempérer ce résultat en rappelant que le nombre de données est relativement faible.

Annexe M : Mots clés [136]

Perte Critique	Résultat	Acteur	
account	availability	(1) *Actions humaines*	(2) *Défaillance technique*
accounting system	available	administrator	defect
address	breach	deadline	hardware
code	breakdown	denial of service	loading
communication	confidential	destruction	malicious code
computer	congestion	devastation	software
computer system	constrain	employee	stress
confidential	control	extortion	system crash
confidential document	delete	forget	(3) *Erreur du processus interne*
consumer information	deletion	hacker, hacked	unauthorized access
data	disclosure	hacking	(4) *Évènement externe*
disk	disorder	human error	Blizzard
document	disruption	infect	Earthquake
file	disturbance	infection	Eruption
hard-disk	encryption	infiltrate	Explosion
hard-drive	espionage	infiltrated	Fire
homepage	failure	key logger	Flood
info(rmation)	false	lapse	Hail
information system	falsification	logic bomb	heat wave
internet site	falsified	maintenance	Hurricane
names	falsifying	malware	Lightning
network	incompatibility	manager	natural catastrophe
numbers	incompatible	manipulate	Outage
online banking	incomplete	miscommunication	pipe burst
payment system	integrity	mistake	Riot
PC	interruption	misuse	Smoke
personal information	limit	omission	Storm
phone	lose	online attack	Thunder
purchase information	loss	oversight	Tornado
record	lost	phish	Tsunami
reports	malfunction	phishing	Typhoon
server	missing	spam	Unrest
site	modification	Trojan	Utilities
SS number	modified	vandalism	War
stored information	modify	virus	Weather
tablet	overload	worm	Wind
trade secret	publication		
webpage	restrict		
website	sabotage		
	steal		
	stole		
	theft		

136. Notons que nous avons ajouté à cette liste les mots qui en sont dérivés, les verbes conjugués, les mots avec tiret ou espace, par exemple : *infos, information, forget / forgot / forgotten, etc.*

Annexe N : Adéquation des lois à la log-distribution des violations empiriques

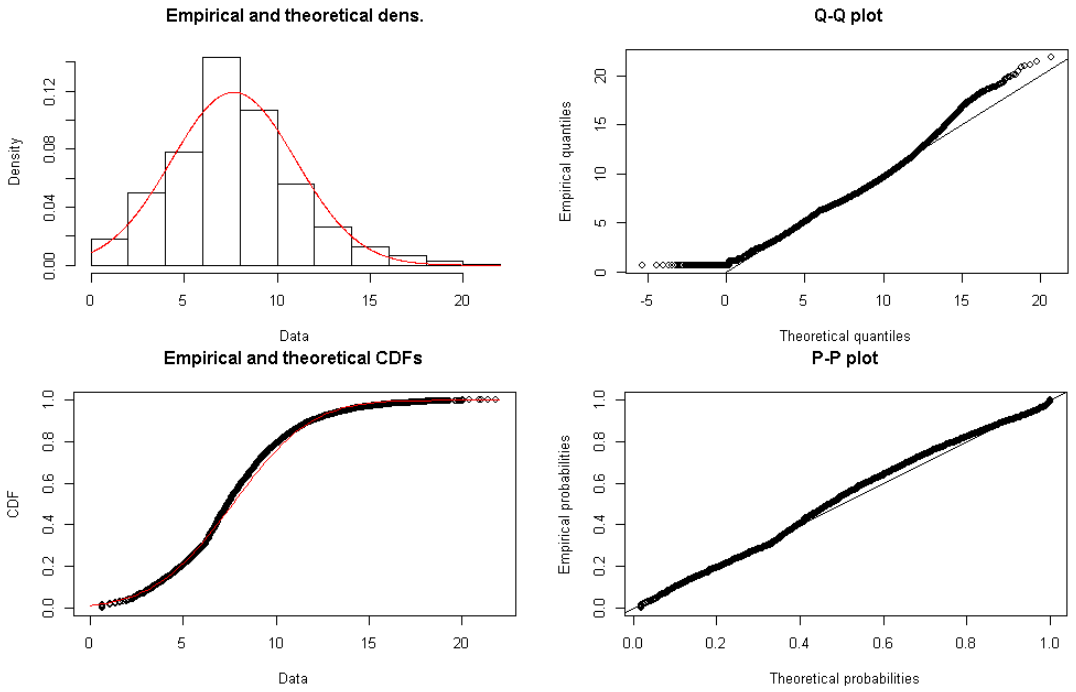


FIGURE 41 – Résumé de l'adéquation de la distribution Normale

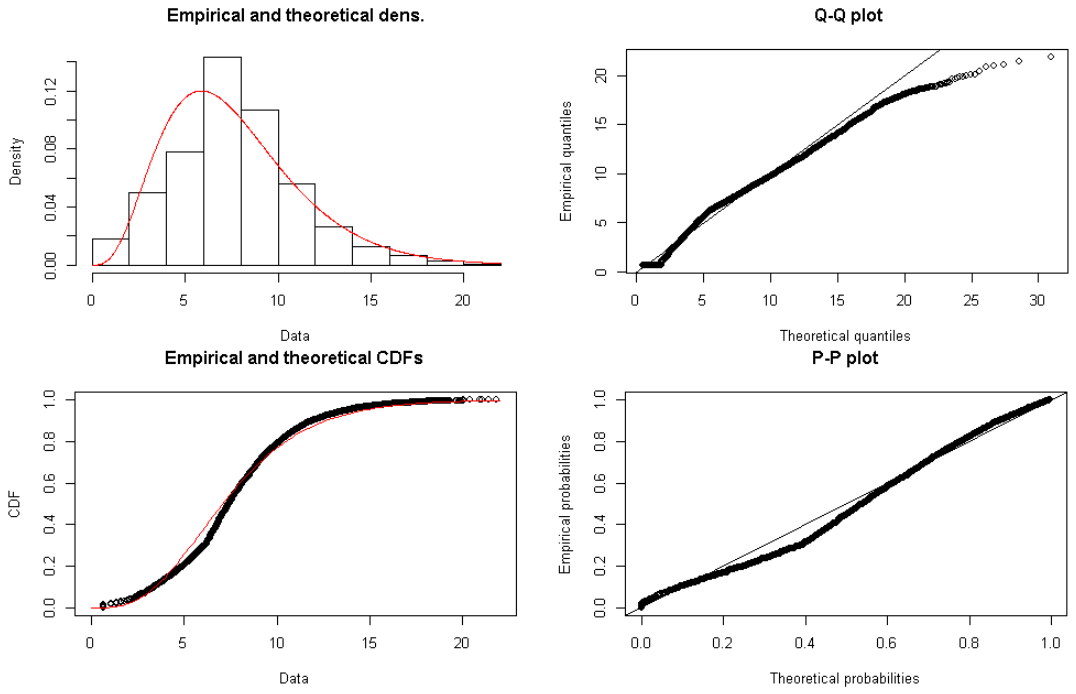


FIGURE 42 – Résumé de l'adéquation de la distribution Gamma

Annexe O : Scénario - pertes assurables additionnelles

Le scénario entraînerait pratiquement certainement des réclamations dans des domaines d'assurance que nous n'avons pas inclus dans cette étude. Prenons par exemple [137] :

Réclamations liées à des blessures

Ce scénario envisage relativement peu de personnes souffrant de blessures corporelles. Or, il est envisageable que des employés dans les usines de production soient blessés par les feux et explosions des générateurs, ou dans la lutte contre les incendies. Des personnes pourraient être blessées dans des accidents résultant de la coupure électrique. Un accident de transport (transport public, aviation commerciale, etc.) pourrait entraîner un paiement d'assurance important pour les blessures, en dommages et intérêts. Les hôpitaux et les maisons de soins infirmiers pourraient ne pas réussir fournir des traitements à la suite d'une perte de puissance. Ces situations pourraient donner lieu à des versements d'assurance au titre de la GAV, accident personnel, indemnisation des accidents du travail, responsabilité civile générale, assurance maladie, assurance vie, etc.

Auto

Les sinistres automobiles résultant d'accidents de la route seraient probablement plus fréquents pendant la période de panne et défaillances des feux de circulation, bien que cela puisse être plus que compensé par la réduction des déplacements en raison de la une réduction de l'activité économique.

Assurance Incendie

La fréquence d'accidents et d'incendies a tendance à augmenter lors de longues périodes de coupures de courant, en partie pour des raisons de sécurité et à cause de la déconnexion des systèmes de prévention (mis hors lignes par le *Black-out*).

Responsabilité environnementale

La panne pourrait entraîner des accidents industriels qui conduirait à la libération de polluants et à l'environnement dommage. Cela pourrait entraîner des paiements importants par assureurs sous couvertures de responsabilité environnementale détenues par les entreprises jugées responsables.

Troubles sociaux

Les pannes de courant passées ont provoqué des émeutes et des troubles sociaux dans les populations urbaines, entraînant des pillages, des dommages, incendie criminel de bâtiments et incendies de voitures. Ce serait générera probablement des pertes de biens pour les assureurs au-dessus des estimations.

137. Source :*"Emerging Risk Report"*, Lloyd's of London 2015

Annexe P : La méthode de Monte Carlo

Afin de générer les valeurs, nous avons utiliser la méthode dite de Monte-Carlo : Supposons que l'on veuille calculer une quantité I. La première étape est de la mettre sous forme d'espérance $I = \mathbb{E}(X)$ avec X une variable aléatoire. Si on sait simuler des variables $X_1, X_2, ...$ indépendantes et identiquement distribuées (iid), on peut alors approcher I par

$$I = \frac{X_1 + X_2 + ... + X_N}{N}$$

avec N "grand", sous réserve d'application de la loi des grands nombres. C'est ce type d'approximation que l'on appelle méthode de Monte Carlo [138].

Nous avons l'expression de l'espérance d'une fonction g de variable aléatoire X, résultat du théorème dit "de transfert", d'après lequel :

$$G = \mathbb{E}(g(X)) = \int_{[a,b]} g(x) f_X(x) dx \tag{8}$$

avec f_X une fonction de densité sur $[a, b]$.
Il est commun de prendre une distribution uniforme sur $[a, b]$: $\mathbb{U}_{[a,b]}$ $f_X(x) = \frac{1}{b-a}$.
Ces formules peuvent être étendues aux probabilité discrètes en sommant grâce à une mesure ν discrète (type Dirac par exemple). L'idée étant de produire un échantillon $(x_1, x_2, ..., x_N)$ de la distribution X (c'est-à-dire d'après la densité f_X) sur le support $[a, b]$, et de mesurer un nouvel estimateur de G dit de Monte-Carlo, à partir de l'analyse de cet échantillon.
La LGN (loi des grands nombres) suggère de déterminer cet estimateur à partir de la moyenne empirique :

$$\tilde{g_N} = \frac{1}{N} \sum_{i=1}^{N} g(x_i),$$

qui se trouve être, par ailleurs, un estimateur sans biais de l'espérance mathématique.

Il s'agit de l'estimateur de Monte-Carlo. Nous remarquons donc qu'en remplaçant l'échantillon par un ensemble de valeurs empiriques prises dans le support d'une intégrale, et de la fonction mathématique à intégrer, nous pouvons déterminer une approximation de sa valeur, statistiquement. Cette estimation est sans biais, dans l'idée où $\mathbb{E}(\tilde{g_N}) = G = \mathbb{E}(g(X))$. Il faut aussi quantifier la précision de cette estimation, par la variance de $\tilde{g_N}$. Si l'échantillon est supposé composé de données indépendantes et identiquement distribuées (iid), cette variance est construite à l'aide de la variance empirique :

$$S^2_{g(X)} = \frac{1}{N} \sum_{i=1}^{N} (g(x_i) - \tilde{g_N})^2 \simeq \sigma_g^2$$

138. La présentation de la théorie sous-jacente à Monte Carlo est issue en partie de *Wikipedia* et *OpenClassroom*, 2019.

avec

$$\sigma_g^2 = \mathbb{E}(g^2(X)) - \mathbb{E}(g(X))^2 = \int_\Omega g^2(x) f_X(x) dx - G^2$$

Par le théorème central limite, on sait que la variable :

$$Z := \frac{\tilde{g_N} - G}{\sigma_g / \sqrt{N}} \mathcal{N}(0; 1)$$

qui est centrée et réduite, suit approximativement la loi Normale centrée réduite, ou loi de Gauss. Il est alors possible de construire des intervalles de confiance, ce qui permet d'encadrer l'erreur commise en remplaçant G par $\tilde{g_N}$. Si cette erreur est dénotée e_n, alors pour un niveau de risque α donnée, on a :

$$|e_n| \leq z_{1-\alpha/2} \frac{\sigma_g}{\sqrt{N}}$$

avec probabilité $1 - \alpha$. Le réel $z_{1-\alpha/2}$ est le quantile de la loi Normale centrée réduite. Par exemple, au niveau de risque $\alpha = 5\%$, on trouve dans les tables $z_{1-\alpha}/2 = 1,96$ et l'erreur est majorée par $1,96\sigma_g/\sqrt{N}$. Cette méthode permet donc de quantifier l'erreur commise, à condition d'estimer σ_g par sa contrepartie empirique :

$$\tilde{\sigma_g} = \sqrt{S^2_{g(X)}}$$

Annexe Q : Le principe de la Kill Chain probabilisée

Au vu des limites des méthodes historiques et des difficultés à proposer des modèles robustes pour la modélisation de la fréquence, des coûts et de l'exposition au risque cyber, les experts développent des techniques alternatives de gestion de cette menace. Il y a plusieurs questions qui restent sans réponses avec les moyens historiques de calculs. Les nouveaux acteurs et idées de mesures du risque ont pour ambition d'apporter une réponse plausible à ces problématiques. Ces interrogations sont diverses et nécessite un travail approfondi, que ce soit dans la probabilité d'occurence (modèle "*Kill Chain*" ou "*Expert*"), ou dans l'empreinte (méthodes de mesure des interconnexions au sein d'un portefeuille) ou encore de l'impact financier).

La *Kill Chain* est un des modèles qui a vu le jour pour répondre à ces problématiques. Il s'agit d'une des possibilités de modélisation de la réussite d'une perturbation cyber. Cette dernière représente le déroulé d'une attaque classique sur un système d'information.

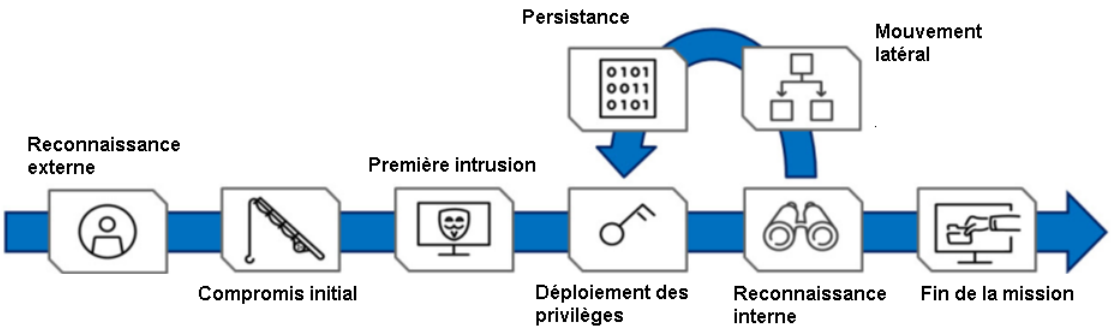


FIGURE 43 – Chronologie d'une attaque cyber

La figure ci-dessus représente les étapes simplifiées d'une attaque cyber. Les principaux paliers seraient donc les suivants :

- **Reconnaissance externe** : Exploiter les renseignements en *OpenData* et pour collecter des données sur la société de distribution visée et identifier les cibles (repérage des lieux, test des moyens de défenses (pare-feu, système anti-intrusion), recherche des vulnérabilités, ...) ;
- **Compromis initial** : Accéder au réseau commercial de l'entreprise de distribution par un "*phishing*" ;
- **Première intrusion** : Déployer des logiciels malveillants sur les systèmes voulus. Configuration de l'infrastructure de commande et de contrôle. Il s'agit du moment où l'attaque devient active. Les *hackers* pénètrent le réseau et installent les virus complémentaires ;
- **Déploiement des privilèges** : Voler les informations d'identification des administrateurs du réseau professionnel à l'aide d'outils spécifiques pour contourner les logiciels antivirus et

autres moyens de défense (modification des certificats pour obtenir des autorisations pour accéder à tous les niveaux de ressource) ;

- **Reconnaissance interne** : Analyser l'environnement interne pour rechercher les systèmes vulnérables et commencez à exploiter les ressources ;
- **Mouvement latéral** : Voler les informations d'identification VPN [139] de l'opérateur pour les faire se déplacer dans le réseau de supervision de l'usine (recherche de l'information désirée) ;
- **Persistence** : Infecter des cibles supplémentaires dans le réseau de l'entreprise avec des "backdoors" (échappatoires) supplémentaires ;
- **Fin de la mission** : Exploiter le "*Wiperware*" pour effacer le MBR (*Master Boot Record* : enregistreur principal) des systèmes d'entreprise et supprimer les connexions sélectionnées : c'est-à-dire sortir en toute sécurité du système de façon à ne pas avoir laissé de trace susceptible de remonter jusqu'à la source.

Cette représentation en frise chronologique n'est pas simplement utile pour comprendre et analyser l'évolution d'une attaque, mais permet également une étude probabiliste de la réussite de chaque étape de cette dernière. En effet, la méthode de modélisation par *Kill Chain* part du principe que l'on estime le taux d'échec à chaque pas de l'intrusion (en fonction des moyens de protection de la cible). La figure ci-dessous représente cette idée avec des chiffres.

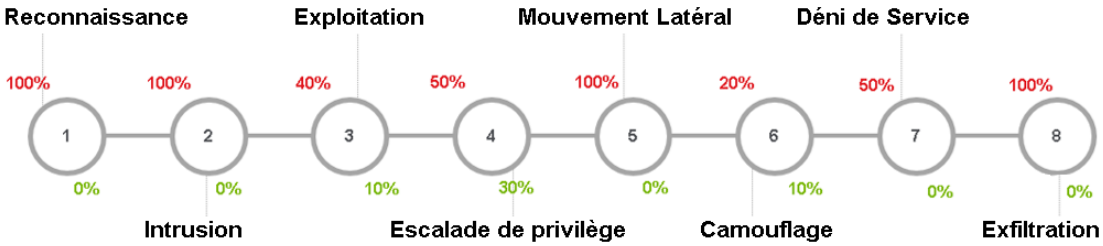


FIGURE 44 – Exemple de chronologie probabilisée d'une attaque cyber

Sur la figure ci-dessus, nous avons afficher en exemple des probabilités de succès de la tentative d'infiltration (en rouge) et le taux de diminution de cette hypothèse d'intrusion par les moyens de défense (en vert). Ainsi, nous pouvons estimer pour cet exemple la probabilité de réussite et donc un taux de réalisation, soit une fréquence.

139. "Virtual Private Network" : système permettant de s'isoler du réseau lorsqu'on échange avec un autre ordinateur

$$\begin{aligned}
\mathbb{P}(\text{intrusion}) &= \mathbb{P}\Big(\bigcap_{i\in I} \text{intrusion}_i\Big) \\
&= \prod_{i\in I} \mathbb{P}(\text{intrusion}_i) \qquad (\textit{Par indépendance}) \\
&= \prod_{i\in I} \mathbb{P}(\text{succès}_i - \text{échec}_i) \\
&= ... \\
&= 0.3\%
\end{aligned}$$

Ainsi nous avons pu effectuer une estimation de probabilité d'occurrence d'une telle perturbation. Pour que ce type de modèle soit effectif, les entreprises qui proposent ces mesures s'allient avec des géants de l'informatique. L'étude des moyens de défense et des parts de marché par ces experts permet de proposer des probabilités d'occurrence des incidents cyber.

Réponses aux autres questions

Afin de pouvoir faire correspondre ces mesures avec une tarification efficace du risque cyber porté par le portefeuille, des scénarios sont construits, adapté au profil de risque. On peut ainsi observer l'impact de chacun des scénarios sélectionnés sur le portefeuille et donc de voir comment ce dernier réagit en fonction du type d'agression (méthode d'introduction, type de perte, durée de l'intrusion, ...). Les scénarios ont trois parties de modélisation :

- **La probabilité** -
  Réponse à la question : "Quelle est la fréquence d'occurrence d'un tel scénario ?"
  → Plusieurs modèles de vraisemblance basés sur des analyses historiques, la modélisation des menaces, l'analyse de la chaîne de destruction et une enquête auprès d'experts. Permet de répondre à la question de la fréquence de l'évènement ;
- **L'empreinte/L'impact** -
  Réponse à la question : "Quelles compagnies dans mon portefeuille sont impactées par ce scénarios ?"
  → Part du marché et méthodologie détaillées pour calculer l'impact par l'interconnexion sur les différentes vulnérabilités des entreprises. Permet de désigner quelles entreprises sont affectées par le scénario imaginé ;
- **Le coût** -
  Réponse à la question : "Quel est l'impact financier associé à ce scénario ?"
  → Les coûts des pertes assurantielles, à partir d'une analyse des composants de la couverture, ainsi que du marché concerné (secteur d'activité, zone géographique, taille de l'entreprise, etc.).

Références

[1] Jean Arlet : Electricity tariffs, power outages and firm performance : A comparative analysis. *In Proceedings of the DECRG Kuala Lumpur Seminar Series, Kuala Lumpur, Malaysia*, volume 23, 2017.

[2] Baruch Berliner : *Limits of insurability of risks*. Prentice Hall, 1982.

[3] Christian Biener, Martin Eling et Jan Hendrik Wirfs : Insurability of cyber risk : An empirical analysis. *The Geneva Papers on Risk and Insurance-Issues and Practice*, 40(1):131–158, 2015.

[4] Rainer Böhme et Gaurav Kataria : Models and measures for correlation in cyber-insurance. *In WEIS*, 2006.

[5] Rainer Böhme, Galina Schwartz *et al.* : Modeling cyber-insurance : Towards a unifying framework. *In WEIS*, 2010.

[6] James L Cebula et Lisa R Young : A taxonomy of operational cyber security risks. Rapport technique, CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST, 2010.

[7] Groupe de Travail IA : Emergence du besoin en cyber assurance. *Institut des Actuaires*, 2017.

[8] Rapports ENISA : National cyber securitystrategies, 2012.

[9] Naomi E Feldman et Bradley J Ruffle : The impact of including, adding, and subtracting a tax on demand. *American Economic Journal : Economic Policy*, 7(1):95–118, 2015.

[10] Sean Foley, Jonathan R Karlsen et Tālis J Putniņš : Sex, drugs, and bitcoin : How much illegal activity is financed through cryptocurrencies ? *The Review of Financial Studies*, 32(5):1798–1853, 2019.

[11] Mehdi Kadivar : Cyber-attack attributes. *Technology Innovation Management Review*, 4(11), 2014.

[12] Stanley Kaplan et B John Garrick : On the quantitative definition of risk. *Risk analysis*, 1(1):11–27, 1981.

[13] Ralph Koning, Nick Buraglio, Cees de Laat et Paola Grosso : Coreflow : Enriching bro security events using network traffic monitoring data. *Future Generation Computer Systems*, 79:235–242, 2018.

[14] Nir Kshetri : Cloud computing in developing economies. *Computer*, 43(10):47–55, 2010.

[15] le club des juristes : Rapport : Assurer le risque cyber. 2018.

[16] Barlow Lyde : Gilbert (2007),". *International Comparative Review of Liability Insurance Law," Insurance Day May*.

[17] Steve Morgan : Cybercrime report, 2017. 2017.

[18] Hulisi Öğüt, Srinivasan Raghunathan et Nirup Menon : Cyber security risk management : Public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection. *Risk Analysis : An International Journal*, 31(3):497–512, 2011.

[19] Rain Ottis : Analysis of the 2007 cyber attacks against estonia from the information warfare perspective. *In Proceedings of the 7th European Conference on Information Warfare*, page 163, 2008.

[20] L Ponemon : Cost of data breach study : Global analysis. *Poneomon Institute sponsored by Symantec*, 2013.

[21] Florian PONS : Etude actuarielle du cyber risque. *Institut des Actuaires*, 2014.

[22] Adam Rose, Gbadebo Oladosu et Shu-Yi Liao : Business interruption impacts of a terrorist attack on the electric power system of los angeles : customer resilience to a total blackout. *Risk Analysis : An International Journal*, 27(3):513–531, 2007.

[23] Michael Rothschild et Joseph Stiglitz : Imperfect information. *The Quarterly Journal of Economics*, 90(4):629–649, 1976.

[24] Innovation Series : Business blackout, 2015.

[25] Scott J Shackelford : Should your firm invest in cyber risk insurance ? *Business Horizons*, 55(4):349–356, 2012.

[26] Babak Shoraka : *An empirical investigation of the economic value of information security management system standards*. Nova Southeastern University, 2011.

[27] Gary Stoneburner, Alice Y Goguen et Alexis Feringa : Sp 800-30. risk management guide for information technology systems. 2002.